

VOLUME 2 (2016) - ISSUE 1

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES



ANALYSES ■ POLICY REVIEWS ■ OPINIONS

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

Chief Editor: Dr Joanna Świątkowska
*CYBERSEC Programme Director and Senior Research Fellow of the
Kosciuszko Institute, Poland*

Honorary Member of the Board: Dr James Lewis
*Director and Senior Fellow of the Strategic Technologies Program,
Center for Strategic and International Studies (CSIS), USA*

Member of the Board: Alexander Klimburg
*Nonresident Senior Fellow, Cyber Statecraft Initiative, Atlantic
Council ; Affiliate, Belfer Center of Harvard Kennedy School, USA*

Member of the Board: Helena Raud
*Member of the Board of the European Cybersecurity Initiative,
Estonia*

Member of the Board: Keir Giles
Director of the Conflict Studies Research Centre (CSRC), UK

Editor Associate: Izabela Albrycht
Chairperson of the Kosciuszko Institute, Poland

Executive Editor: Matylda Kuchnik
Designer: Paweł Walkowiak | perceptika.pl

Proofreading:
H&H Translations | hhtranslations.com.pl

ISSN: 2450-2111

The ECJ is a quarterly journal, published in January, April, July and October.



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

**Printed in Poland
by Drukarnia Diament | diamentdruk.pl**

DTP: Michał Walczak

Citations: This journal should be cited as follows:
"European Cybersecurity Journal", Volume 2 (2016), Issue
1, page reference

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.

© 2016 The Kosciuszko Institute
All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.

EDITORIAL



DR JOANNA ŚWIĄTKOWSKA

Chief Editor of the European Cybersecurity Journal

CYBERSEC Programme Director

Senior Research Fellow of the Kosciuszko Institute, Poland

The year 2015 brought a lot of very interesting events in the area of cybersecurity. In Europe, there were many negotiations connected with key regulations, such as NIS Directive and the General Data Protection Regulation. We have witnessed the development of new threats and network utilisation, e.g. in the context of the conflict in Ukraine. Cybersecurity has also become an important subject of discussions for major global actors. The second edition of European Cybersecurity Journal (ECJ) refers to the events of the past year and it provides analysis of the trends and processes that will be crucial in the near future.

The ECJ is opened up by a short summary of European Cybersecurity Forum 2015 – CYBERSEC 2015 – international conference dedicated to strategic challenges for Cybersecurity, inaugurated in September in Kraków. The conference hosted 400 participants including 120 experts and policy makers from around the world, who worked on substantive recommendations.

A brief text written by Jarno Limnéll of the Finnish Aalto University, which draws attention to the need to build a European system of cybersecurity, also refers to this event.

From the point of view of modern states, the conflict in Ukraine showed how important it is to provide safe functioning of the cyberspace and in how many ways cyberspace can be used to hostilities. The Ukrainian policy in the area of cybersecurity describes the text written by Oleksandr Potii of JSC Institute of Information Technology. This is an important material which helps understanding the way of looking at cybersecurity of this country.

Hostile acts in cyberspace can very quickly escalate and lead to dramatic consequences affecting the stability of the entire international community. For this reason, issues related to standards of operation in cyberspace and confidence-building have become an inherent part of the dialogue at the international level. In 2016, Germany will take over the OSCE Chairmanship. Karsten Geier from Federal Foreign Office of Germany describes in his text that talks about dialogue, confidence and security in cyberspace will play an important role under the German presidency.

The second issue of the quarterly provides also a series of different and interesting perspectives on analysing the role of the state in creating a safer cyberspace. Texts written by Rafał Magryś from the company Exatel and Rob van Kranenburg who is a founder of the think-tank The Internet of Things, show two approaches - one relating to specific solutions, and the other one focused on a broader perspective.

The analysis of Izabela Albrycht, chairperson of the Kosciuszko Institute, completes these insights by pointing to the need for a state to engage in issues of widely understood cyberspace. She also draws attention to the deepening deficit of professionals dealing with the protection of cyberspace.

In turn, Piret Pernik from the Estonian International Centre for Defence and Security presents the Estonian approach to cybersecurity by depicting Estonian innovative initiatives such as the E-Residency Date Embassies.

Text written by Rolf H. Weber of the University of Zurich, which examines issues of competitiveness and innovation in the Digital Single Market, completes the analysis of European initiatives.

The second number of ECJ provides also texts containing very specific recommendations in the area of cybersecurity,

enabling us to understand the functioning of specific mechanisms. In this context, it is worth paying attention to the material prepared by Tomasz Niewdana from Fortinet, which refers to the issue of the Advanced Attacks and Integrated Defence. At this point, it is also worth mentioning the text written by Artur Kofosowski, which explains the way of looking at cybersecurity and the computerisation of the largest Polish reinforcing company called Armament Group. The material prepared by Agnieszka Wiercińska-Krużewska from WKB law firm presents a very high level of added value. The author conveys very specific recommendations on how private companies should deal with cybersecurity.

Last but not least, we want to continue a tradition launched in the first issue. Hence, the second issue of the quarterly includes an interview with Marcin Libicki from the RAND Corporation, who is one of the most renowned American experts in the field of cybersecurity.

We kindly invite you to read the following publications, which will not only bring portions of expertise, but also inspire for further exploration of various aspects of cybersecurity.

Joanne Siskind

CONTENTS

7

EUROPEAN CYBERSECURITY FORUM 2015 – CONCLUSIONS AND RECOMMENDATIONS

Dr Joanna Świątkowska

15

INTERVIEW WITH DR MARTIN LIBICKI

18

NORMS, CONFIDENCE AND CAPACITY BUILDING: PUTTING THE UN RECOMMENDATIONS ON INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE CONTEXT OF INTERNATIONAL SECURITY INTO OSCE-ACTION

Karsten Geier

24

THE ROLE OF THE STATE IN CREATING THE SAFE CYBERSPACE AND ITS ATTITUDE TOWARDS THE INTERNET OF THINGS

Rafał Magryś

28

FRAMEWORK OF UKRAINIAN NATIONAL SYSTEM OF CYBERSECURITY

Prof. Oleksandr V. Potii

38

CYBER TECHNOLOGIES

Artur Kołosowski

41

EUROPEAN CYBERSECURITY MUST BE STRENGTHENED

Prof. Jarno Limnéll

43

**EDUCATION AS A KEY FACTOR IN THE PROCESS OF BUILDING
CYBERSECURITY**

Izabela Albrycht

49

HOW SHOULD PRIVATE COMPANIES DEAL WITH CYBERSECURITY?

Agnieszka Wiercińska-Krużewska

54

E-RESIDENCY AND DATA EMBASSIES: A COUNTRY WITHOUT BORDERS

Piret Pernik

62

ADVANCED ATTACKS AND INTEGRATED DEFENCE

Edited by: Tomasz Niewdana

67

**WANTED: A PRAGMATIC CYBERNETICS AND A NEW ELITE.
A NEW FORM OF POLITICS IN CONTEXT OF THE TECHNOLOGICAL
CHANGES OF INTERNET OF THINGS**

Rob van Kranenburg

72

COMPETITIVENESS AND INNOVATION IN THE DIGITAL SINGLE MARKET

Dr Rolf H. Weber



EUROPEAN CYBERSECURITY FORUM 2015 – CONCLUSIONS AND RECOMMENDATIONS



DR JOANNA ŚWIĄTKOWSKA

Dr 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.

1. Introduction

European Cybersecurity Forum 2015 – CYBERSEC 2015 – was the first edition of annual and international conference dedicated to strategic challenges for Cybersecurity, inaugurated in September in Kraków. The event hosted 400 participants, among the others 120 decision-makers, experts and academia from all over the world, actively engaged in substantive work before and after the conference. During CYBERSECForum, we prepared eight Breakout Sessions under four thematic panel discussions accompanied by several additional events. During the preparation for the conference we also organised eight webinars. Throughout the whole process, we have developed number of conclusions and recommendations which can serve for different groups of stakeholders in order to build a variety of cybersecurity system components in their area of operations. This article hereby presents an analysis of the most important topics and arguments that have been raised during debates at CYBERSEC Forum. The analysis contributed to aggregation of key conclusions and presentation of a summary.

2. The crucial role of a state

One of the common points in all the discussions that took place at CYBERSEC Forum was a belief that the role of activities related to cybersecurity is strategic importance. Regardless of whether we think of cybersecurity at the level of a single private entity or at the state level, the key issue is to make it a challenge which is built into the strategy of the functioning of the whole organism. Supervision and control should be assigned to the highest level of both political responsibility and the board company. Only if crucial decision makers realise how important cyberspace is for functioning of the company or the state, we will have a chance to take effective actions and decisions concerning allocating adequate financial resources. The participants of the conference indicated that providing an adequate level of cybersecurity is a direct function and responsibility of countries (in a macro scale) and individual enterprises (in a micro scale). Regardless of the important supporting role supranational organisations such as NATO or the EU,



STATE
STREAM



MILITARY
STREAM



FUTURE
STREAM



BUSINESS
STREAM

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

these are countries which face the need to build their own capabilities and solutions to ensure their safe operation in cyberspace. Supranational structures can harmonise approaches, indicate correlation and provide help. However, these are states which must take responsibility for proper preparation face cyberthreats. Similarly, states can support private entities, even those which are crucial to country's security. However, private entities cannot rely only on states and they should take care, in first place, for their own safe operation. Such a clear identification of responsibility entails postulate for fair implementation of appropriate measures or proper allocation of a large budget for cybersecurity.

The postulate for building capacity in the field cybersecurity went hand in hand with speakers' insights that there is a general tendency to build and apply national solutions, particularly in the most sensitive areas of the state. In other words, the greatest emphasis is placed on ensuring control over hardware, software, in order to maximise the level of security. In dealing with external suppliers it was recommended to take precautions and select trusted partners whose products are testable. This trend has been noticed on two levels – national and regional, where one of participants also recommended the implementation a more pragmatic approach.

Speaking of private companies exposed primarily on the activities of cybercriminals, participants pointed out that despite the help they can get from the state, first of all, they should take care of their own safety themselves. What is more, they should take more proactive actions, not based solely on the use of passive defence, which rely on active countering threats. Increasing situational awareness and information sharing should be standard practices in the organisations.

3. Protection of critical resources

There was a call for promoting the use of proactive approach at the state level and individual companies, as well as the implementation of the action-oriented goal. In order to effectively build cybersecurity, one should know threats and the reasons for which it is protected. Effective fight against cyberthreats requires

implementing effective risk management system.

First of all, we should clearly identify and analyse the most valuable and critical resources, understand the risks, and then on that basis we should implement appropriate action. Countries and companies should also better understand the risks and consequences that may threaten them. For this reason, the aim of actions must be clearly defined.

The postulate reported during a session dedicated to cybersecurity of critical infrastructure was a good illustration of the process of understanding our own resources. One of the participants pointed out that even within the critical infrastructure, not all elements are critical, and therefore we should require different levels of activities aimed at providing security. For this reason, one must identify the most important elements and spend most of widely understood efforts for their defence.

4. Education

While building capacity for cybersecurity, countries should meet deepening problem of shortages of specialists. There are increasing needs in both the private and public sector in the field looking foremost skilled cybersecurity professionals. Therefore, we need to start building strategies for professional forces at national level. The supply should result from market needs, and universities in consultation with the private sector should adapt to this strategy of education. The common denominator of almost all the sessions was the issue of increasing awareness and education on cybersecurity. It is not only about learning the aforementioned specialists. Our objective should be focused on increasing citizen awareness in terms of "hygienic" and safe use of the network, and equipping them with basic knowledge in this area. That is why, one of the postulates highlighted that cybersecurity should be incorporated in all educational cycles from an early age. Ministries of Education of all EU countries should deal with this issue.

5. Funding

Financial issues were one of the most important parts of discussions at CYBERSEC Forum. Participants unanimously pointed out that spending on cybersecurity must be increased. More and more

countries decide to increase the level of defence spending, for example by introducing the principle of designating 2% of their GDP for this purpose. One of the suggestions was to reserve a specific, substantial part of the budget just for the aspects related cybersecurity, both within countries and international organisations. In addition, participants suggested increasing the expenditure on cybersecurity not only in the military sector, but also in the civilian one. The budget expenditure for this purpose should be clearly increased.

Some of these expenses should be spent on conducting broad Research & Development activities in the area of cyberspace. As participants pointed out, there are national and supranational funds (EU) supporting these activities. However, they are not yet sufficiently utilised. It was also recommended that in order to successfully apply for financing, firstly, we need to ensure rapid commercialisation projects. What is more, participants agreed that private entities along with the public ones should work on prioritising public spending, and a special fast path should be earmarked for small and medium-sized enterprises. In this context, there was also an important postulate to support European start-ups and their capabilities so that they could carry out their activities in Europe, and did not have to emigrate in order to seek funds. Participants, with respect to good practices in framework of public-private co-operation and financing actions, pointed out several European initiatives such as NIS Platform, Cybersecurity Private-Public Partnership (within DSM), which offer stakeholders many opportunities.

6. Information sharing

A large part of discussions during many session at CYBERSEC Forum was dominated by the topic related to the exchange of information both at the level the private- public sector and within the private sector itself. These activities have been identified as the foundation of providing cybersecurity and the basis for proactive action. During the discussions there were several recommendations concerning methods of ensuring the effectiveness of this process participation of all stakeholders. The table below presents the most important postulates:

EFFECTIVE ELEMENTS OF INFORMATION SHARING
<ul style="list-style-type: none"> • Shared information must in a real way contribute to the solving of pre-defined problems. Stakeholders must know what kind of information is needed and why (what kind of problem will be solved) this can be called targeted information sharing.
<ul style="list-style-type: none"> • Co-operation and information sharing must work as a win-win model. Information from the public sector should be shared on equal basis with those from the private one. The current state of affairs, when public information is excluded from dissemination, is perceived as unfair. This must be a two-way process, and private sector must be an equal part of the system.
<ul style="list-style-type: none"> • Governments should provide a clear plan for processing the security data obtained from private sector, and based on this data, they should provide effective input into the cybersecurity dialogue. All the parties involved must see clear results of the co-operation.
<ul style="list-style-type: none"> • States should play an important role in information sharing process during a crisis situation.
<ul style="list-style-type: none"> • Information must be relevant and timely
<ul style="list-style-type: none"> • The absolute precondition of successful information sharing is protection of privacy and sensitiveness of information. Actors, which are involved must be convinced that exchanging information will not harm their business and their clients.

The effective information sharing is perceived as a key to provide the security of critical infrastructure. Another key action in this area is the application of appropriate standards. Cybersecurity standards should be developed at the sectorial level and applied rigorously.

7. Public - Private Partnership

During the discussions there were different opinions whether a private-public co-operation and the application of standards should be governed by mandatory laws or rather based on a voluntary approach. The collision of these two approaches was evident not only in regard to the protection of critical infrastructure, but practically in all subjects discussed at CYBERSEC Forum. The supporters of the mandatory laws argued, inter alia, that cybersecurity often plays too important role to let entities or forces of the free market decide. The proponents of the voluntary approach indicated that the sanction approach often leads to minimum service obligations and it does not solve the real problems. Moreover, the solutions proposed by the public sector do not keep up with the changing environment.

Although the dispute was not solved during CYBERSEC Forum, and it is difficult to refuse certain rights of each parties, we believe that maybe it would be worth looking for intermediate solutions that would solve at least part of the dilemma. If within each body, including the state, not every component is critical, and at the same time there are some components responsible for the functioning of the whole body, then maybe it is worth applying a flexible approach, and use sanction approach where necessary. Then, the effects problems would have larger social repercussions.

Regardless of the approach, it is worth using properly constructed system of financial and non-financial incentives to mobilize the private sector to co-operate and provide adequate cybersecurity. This issue is likely to become one of the subjects of discussion at next CYBERSEC Forum.

8. Strategic international co-operation and military aspects

One of the elements, which was approved by the participants, was a demand for more intensive implementation of the exercise refining activities in the

field of cybersecurity. There was a recommendation for intensified exercise at both national and international levels. One of the postulates also spoke about organising joint exercises of NATO and the EU, especially in the face of rising hybrid threats. Exercises allow you to test many elements of an effective defence, among others, procedures and information sharing.

In the context of the talks on cybersecurity in the Military session, participants raised many of the key issues, which are important to national defence and also allied co-operation, mainly in the activities of NATO.

The other part of the debate concerned the observed trend associated with building strategies and doctrines of cybersecurity. It was considered that the documents of this type should be strictly established, but they should be treated only as the first step in the whole process operations. We need to develop further implementing efforts, primarily, we need to expand the capacity for effective action and preparation procedures for taking concrete actions both in terms of military operations in cyberspace and in relation to emergencies.

The offensive abilities of modern army to operate in cyberspace were discussed in detail. Many experts indicated that the expansion of this item is necessary. This element is also an important factor in terms of deterrence and proportional defence. According to one of the participants – inability to offensive operations in cyberspace may lead to the fact that in order to respond to the attack we will be forced to go for conventional measures.

For many reasons, operations carried out in cyberspace can lead to the escalation of crises. Cyberspace environment has some features (such as difficulties in attribution), which promotes the development of such adverse events. For this reason, it was pointed out that one should maintain as much transparency as possible in terms of building a cyberdefence policy at the state level. Strategies and doctrines should be fully transparent in order to reduce the risk of misinterpretation of the actions.

Another key instrument that increases confidence in the functioning of cyberspace are CBMs. There was a strong postulate to create and implement them both at the global and regional level.

It was also noted that building capacity at the state level is an important factor, and even a duty, from the point of view of safe operation of the Alliance. Strong member states contribute to strong Alliance. At the same time it should be remembered that currently NATO does not allow to conduct offensive operations in cyberspace within the Alliance, and the decision to expand the offensive capability should be responsibility shouldered by the Member States. In order to meet the postulate of strengthening national actions, participants called on Member States to sign the second generation of Memoranda of Understanding (MOUs).

Participants pointed to the many opportunities and actions that can be taken by NATO in order to strengthen its own capacity. It was recommended to create NATO Specialised Cyber Defence Force operating in a manner similar to the NATO Response Force. Another specific indication was to create Cyber Command Component aside from the Existing Land, Air, Maritime and Special Operations Component Commands.

In the context of discussions on cybersecurity in the military area, once again there was an issue concerning co-operation of private - public sectors. An interesting part of the discussion was to identify the potential and opportunities arising from the formation of volunteer civil defence leagues in which civilians support the activities of the State in the field of cyberdefence. Regarding co-operation with public sector, there were recommendations for further development and promotion of initiatives such as the NATO Cyber Industry Partnership. Similar arrangements should be also considered from the point of view of individual countries.

It was also noted that Member States as well as NATO, should increase their situational awareness in order to operate more effectively in cyberspace. One of the elements leading to this goal is the expansion of capacities in the area of cyberintelligence.

Another important element of the discussion was to indicate that actions in cyberspace conducted by the states (or actions inspired by states) are almost always associated with conventional operations, which are part of measures leading to implementation of specific policy goals. Therefore, effective protection against them requires analysis of the current geopolitical situation and the application of measures belonging range of classic policy. In this context, there was a very important postulate to build the capacity of individual countries within the so-called cyberdiplomacy. Diplomatic corps should have the ability to use variety of tools for all major aspects of cyberspace, including those related to potential conflicts.

The issue of building capacity for taking actions in cyberspace in conjunction with cyberdiplomacy was raised in the context of helping developing countries. In order to think about strengthening cybersecurity at the global level, it is necessary to support these entities, which are at starting point of intensive functioning in cyberspace, and soon they will be its key users. It was pointed out that issues dedicated to cyberspace should become an important element of the development policies in modern states.

Participants in the framework of discussion also raised a need to work in partnership with developing countries on the future of Internet governance. All participants agreed on the fact that we should keep the current, multi-agent network management system. However, we should engage developing countries in the participation within this system.

It was also noted that the management of the Internet, seen from the perspective of actions aimed at cybersecurity, should be based also on the principles of multi-stakeholder approach, and the first action should be to clearly define the roles and responsibilities of all players.

The issues relating to emerging megatrends such as the Internet of Things were important part of the talks during CYBERSEC Forum. Participants pointed to the opportunities and the risks that go hand in hand with these processes. In the face of massive spread of the Internet of Things we were cautioned against placing on the market cheap and untested products, which do not meet safety requirements. It was also indicated that

the Internet of Things implications will have an impact, among others, on employment issues, responsibility for security and other processes such as categorisation of customers.

During the CYBERSEC Forum we had also an opportunity to take part in a special session dedicated to the fight against cybercrime. The main postulates raised during this session concerned the need to build international co-operation, promotion of signing and ratification of the Budapest Convention and its robust implementation into national law, update legal solutions, reinforcing (e.g. by training, exercises or by application of modern technologies) national capacities in terms of prosecution and punishment cybercriminals. Co-operation in this area should take the form of multilateral (e.g. Europol) and also bilateral agreements. Also in this area, participants raised need to build public-private co-operation. Without this component, the effectiveness of the fight against cybercrime is much lower.

9. Conclusion

CYBERSEC abounded in many interesting conclusions. The key recommendations should be implemented as soon as possible, in order to really enhance the level of cybersecurity. Within the framework of the Kosciuszko Institute we will be intensively promoting them among the key target groups. At the same time we will be monitoring critical processes by verifying which of the recommendations were failed to be implemented in real life. On the basis of this action we will specify the status quo and challenges that must be taken when working in a future edition of CYBERSEC Forum. We believe that our work will contribute to improving cybersecurity level in a real way. ■

KARSTEN GEIER
Head of the Cyber Policy Coordination
Staff in Germany's Federal Foreign Office



From left:
MACIEJ JANKOWSKI Deputy Minister of National Defence, Poland
SORIN DUCARU Assistant Secretary General of NATO for Emerging Security Challenges
JURAND DROP Secretary of State at the Ministry of Administration and Digitization, Poland



AMBASSADOR SESSION

ALEXANDER KLIMBURG
Senior Fellow, Atlantic Council / Hague
Centre for Strategic Studies



PAUL NICHOLAS
Senior Director at Microsoft HQ Redmond



CYBERSEC AUDIENCE

EUROPEAN CYBERSECURITY FORUM

Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

26-27 September 2016, Kraków, Poland



CYBERSEC 2016

STAY TUNED

INTERVIEW WITH MARTIN LIBICKI



DR MARTIN LIBICKI

Dr Martin Libicki (Ph.D., U.C. Berkeley 1978) has been a distinguished visiting professor at the U.S. Naval Academy and a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. In addition he is a Distinguished Visiting Professor at the U.S. Naval Academy and has been an adjunct at Columbia University and Georgetown University. He wrote two commercially published books, *Conquest in Cyberspace: National Security and Information Warfare*, and *Information Technology Standards: Quest for the Common Byte* and has a cyberwar textbook (*Cyberspace in War and Peace*) at the publisher's (U.S. Naval Institute Press). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, *Cyberdeterrence and Cyberwar*, *How Insurgencies End* (with Ben Connable), and *How Terrorist Groups End* (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

Dear Mr. Libicki, thank you again for finding time for this interview. We are currently witnessing a very interesting process in which both national and international decision-makers are trying to find most efficient ways to address cyberthreats. Especially in the USA numerous activities regarding domestic and international issues are being undertaken. I would like to talk about them in more details.

In a recent testimony from March 2015 presented before the House Homeland Security Committee, you shared your views on broad range of issues related to information sharing. The main conclusion was that even though this process is of high importance, its implementation itself will not solve all the problems. National cybersecurity is a multidimensional problem. What are the other important elements of this endeavour that should gain attention and be encouraged?

Information sharing is good, but we should not be hung up about the form it takes. Some thoughts:

- a. We need an ethos in the Cybersecurity community that makes not sharing unethical. In the medical community, doctors commonly share (anonymised) information about patients as a way of discussing situations and treatment options, both those that worked well and those that did not. In the aeronautics industry all incidents are reported and the U.S. NTSB was instituted as a fact-finding but not fault-finding investigative body.
- b. We also need an information-sharing mechanism that can infer indications and warnings of a wide attack from the detection of small ones – but there has to be a great deal of empirical work before we understand how.

There is another issue that I would like to underline here. The machine controls essential to critical infrastructures (such as electric power) should be electronically isolated from the rest of the world and

such isolation should be mandated and periodically tested.

In your work you pay a lot of attention to the problem of crisis and its escalation in cyberspace. In this context, I would like to ask you following question. It is a well-known fact that NATO is currently looking for an “adequate” answer to cyberattacks, both the ones which can be treated as the acts of cyberwar and the ones which are below the cyberwar threshold. During the CYBERSEC 2015 Conference, one of the speakers pointed out that in order to have a chance to respond to cyberattacks in a proportional way, the Alliance must develop offensive cyber capabilities. Otherwise, we might end up with conventional tools only, while choosing reaction. What do you think about this approach in context of your research?

A proportional response is itself a reaction. Two overarching issues must be addressed in the context of NATO. First, what can NATO countries tolerate in terms of attacks? Cyberattacks (as opposed to cyberespionage) have yet to create very high damages even when summed (perhaps under \$100m a year). By contrast, conventional war is several orders of magnitude more expensive. What are the risks that by starting with a response to something that takes place only in cyberspace one ends up with something much more serious? Second, if we are talking about Russia, any response has to support NATO's overall posture with respect to that country; cyberspace cannot be considered in isolation.

In one of your numerous excellent papers, one particularly important sentence can be found. You wrote that “cyber operations can supplement war, but they cannot be the war”. It is often forgotten that cyberattacks mostly enhance use of traditional tools (both military and political). Cyberspace can be utilised in a different ways, for instance the example of Ukraine conflict indicates that cyberspace can be used as an element of information warfare. Correct me if I am wrong, but it seems to me that the US underestimated this form of conflict in the past and focused rather on “hard” aspects of cybersecurity. Should it be changed in the future? How to deal

with information warfare carried out in cyberspace?

In the 1990s, the concept of information war encompassed both psychological operations and hacking – despite vast differences between them. And whereas there are circumstances under which hacking can support psychological operations, they are limited circumstances. That said, both psychological operations and hacking may serve parallel strategic purposes, but that still needs to be worked out.

It is widely acclaimed fact that norms of behaviour can influence and shape global environment also when it comes to cyberspace. What are the most important aspects of particular countries' behaviour in cyberspace from the point of view of the US? Which international acts should be normalised in the first place?

The primary US goal is a norm that de-legitimises economically-motivated cyberespionage. A secondary US goal is a norm that forbids cyberattacks on critical infrastructure. The problem is less one of norms as such (after all, President Xi agreed to the first one), but agreement on how violations of such norms should be detected and acknowledged.

Presidential campaign in the US speeds up. Is cybersecurity an important element in candidates' programs? If yes, which aspects play crucial role?

Cybersecurity is playing a somewhat larger role in this year's Presidential campaign. Senator Webb mentioned it (Chinese cyberespionage, mostly) prominently in his remarks during the Democratic candidate debate, but no one followed up. Some Republican candidates bring it up when arguing that the United States is coddling China. Once the Democrats and Republicans stop debating among themselves and debate each other, the issue may arise more strongly.

In September President Obama and Chinese President Xi Jinping announced a new cybersecurity agreement. Later on it was announced that the Chinese government arrested hackers at the request of the US government. What is the importance of the agreement, and can it be a real game changer when it comes to rather tense cyber US-Chinese

relations?

The agreement is significant for giving the United States a basis on which to threaten China if it continues economically-motivated cyberespionage (whereas, before, it would have been enforcing a norm that the Chinese never signed onto). However, as noted above, we have no norms for detecting and acknowledging norms violations. China has always denied cyberespionage whether of the sort that the United States deems illegitimate or of the sort that the United States itself, is accused of doing. As for the arrests, I would need to see more information.

Thank you very much for this inspiring interview. In the upcoming issues of the ECJ, we will elaborate on issues you pointed out. ■

*Questions by:
dr Joanna Świątkowska*

ANALYSIS

NORMS, CONFIDENCE AND CAPACITY BUILDING: PUTTING THE UN RECOMMENDATIONS ON INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE CONTEXT OF INTERNATIONAL SECURITY INTO OSCE-ACTION



KARSTEN GEIER

Karsten Geier is head of the Cyber Policy Coordination Staff in Germany's Federal Foreign Office. He has served in South-Eastern Europe, Brussels (at Germany's Representation to the European Union) and Washington, D.C. (including as exchange officer in the U.S. Department of State). His most recent assignment abroad led him to New York, where he helped set up the European Union Delegation and subsequently worked at Germany's Mission to the United Nations. Karsten was Germany's member of the 2014/2015 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. He also represents his country in the OSCE's Informal Working Group on the Risk of Conflict Stemming from the Use of Information and Communication Technologies.

Numerous states are pursuing military cyber capabilities. The United Nations Institute for Disarmament Research, in its 2013 Cyber Index, found on the basis of publicly available information that there were 114 national cybersecurity programs worldwide. According to this index, 47 states have cybersecurity programs that give some role to the armed forces. These cyber capabilities are affecting international security. They can create real damage in the physical world. In the interest of international peace and security, diplomats and security experts have to ask themselves how to respond, and how effective are their approaches to global cybersecurity.

Cyber capabilities pose a conceptual problem to established security strategies. Traditional political-military strategies predate the existence of the internet. During the Cold War, the opposing parties

built their defence on the idea that the best defence is to deter an enemy state from attacking. Deterrence requires the consequences of any attack to be clearly and credibly communicated ex ante to any potential adversary. This may not hold in cyberspace: perpetrators show great skill in hiding or confusing their targets, using botnets, convoluted routings, delayed messaging and other techniques. They may not even be states. The effort required to attribute cyberattacks, the limits on forensic capabilities, and the absence of co-operation and collaboration between nations tax the credibility of attribution. Consequently, uncertainty about the origin of hostile cyber action is a characteristic of cyber incidents. This makes it difficult for the states to threaten negative consequences of such action. Under such circumstances, deterrence may not work. If political-military strategies fail to account for

cyber capabilities, arms control offers no easy way out, either: Arms control treaties are typically concluded between a finite number of state-actors on a definable military good. By comparison, it seems almost impossible to negotiate an arms control or even disarmament treaty for “cyber weapons”, given the potentially unlimited number of actors, state and non-state, that can develop, procure and proliferate computer malware. Also consider the difficulty defining a “cyber weapon” in the first place: For some, this might be computer malware which allows intruding into another party’s computer system, either with the purpose of conducting cyberespionage, or for cyber sabotage. Others prefer talking about “information weapons”, a much wider term that covers the capacity to threaten, destroy or in other ways affect individuals, society, the state and their interests. A common understanding of what we are talking about remains elusive.



Lessons learned over decades of efforts to stem the international arms race may help us develop effective approaches to global cybersecurity.

Nevertheless, some lessons learned over decades of efforts to stem the international arms race may help us develop effective approaches to global cybersecurity. There are three lessons in particular states should heed:

1. Agree *rules* for state use of cyber capabilities, or more broadly, for responsible state behaviour in cyberspace;
2. Enhance actors’ *confidence* that states will respect these rules.
3. Help other *actors build cybersecurity capacity*.

Since 2005, the United Nations General Assembly has mandated a series of groups of governmental experts (GGE) to work on this issue. The key point of the 2012/2013 Cyber GGE was the following: “*International law, and in particular the UN Charter, is applicable and essential to maintaining peace stability*

and promoting an open, secure, peaceful and accessible ICT environment.” On this basis, the General Assembly requested another GGE in December 2013 “*to study, with a view to promoting common understandings, existing and potential threats in the ICT sphere and possible co-operative measures to address them, including norms, rules or principles of responsible behaviour of states and how international law applies to the use of ICT by states*”.

The 2014/2015 GGE completed its work in June 2015. In its report to the UN Secretary-General, it offered a list of non-exhaustive views on how international law applies to the use of ICTs by States. This list addresses, inter alia, issues of:

- Jurisdiction over ICT infrastructure;
- State sovereignty;
- The inherent right of states to take measures consistent with international law and as recognised in the UN Charter;
- Where applicable, the principles of humanity, necessity, proportionality and distinction;
- The use of proxies;
- International obligations regarding internationally wrongful acts.

The GGE also recommended a number of voluntary, non-binding norms of responsible State behaviour for consideration by States. Such norms do not seek to limit or prohibit action that is otherwise consistent with international law; they reflect the international community’s expectations, set standards and allow the international community to assess the activities and intentions of States. The GGE recommendations include norms on:

- Co-operation to increase stability and security in the use of ICTs;
- Responses to ICT incidents;
- Preventing of the use of a State’s territory for internationally wrongful acts;
- Co-operation concerning terrorist and criminal use of ICTs;
- Respect for human rights while ensuring the secure use of ICT
- Not conducting or allowing ICT activity that intentionally damages critical infrastructure;
- States’ measures to protect their critical

infrastructure from ICT threats;

- Responses to requests for assistance in mitigating malicious ICT acts;
- The integrity of the supply chain, so that end users can have confidence in the security of ICT products;
- Reporting of ICT vulnerabilities and information on available remedies;
- The role of CERTS.

In addition to these norms, the GGE proposed a list of voluntary confidence-building measures to enhance trust and co-operation and reduce the risk of conflict.

The question now is how to take this work further. Various propositions have been brought forward, for example:

- Convene another GGE;
- Establish an open-ended working group;
- Take the matter into the Geneva Conference on Disarmament.

The idea of convening another GGE has found its way into the recommendations of the 2014/2015 report, and a resolution to this end is being discussed in the UNGA's First Committee as we speak. There are good reasons for following this recommendation: The 2014/2015 GGE felt a need to continue the discussion. The GGE format has proven to be successful. The Secretary-General can select the most qualified government experts, ensuring subject-matter expertise. However, important points can also be fielded against yet another GGE: The reports of the four cyber-GGEs since 2004 have become successively more complex and detailed; the process may have explored all possible room for consensus so that immediately convening another such a group may not lead to progress. A problem is also that GGEs comprise a limited membership and therefore may not be perceived as representing the international community as a whole. At some point in the future, we can expect the GGE process to reach the end of its useful life. Until that time, Germany will do its level best to help support the work of the cyber GGEs.

What about establishing an open-ended working group? Such a body, which could be convened under the First Committee of the General Assembly, could be made accessible to all Member States that wish

to contribute. This would address the concerns about inclusiveness. On the other hand, the large membership and the open-ended nature of the mandate would mean that consensus would be very hard – nigh impossible – to achieve. And where would such a group start? Would it build on the reports of the GGEs? Or would it begin anew, undoing hard-won progress? Finally, there is a tension between demands for inclusiveness and the need for expert knowledge in a field as complex and technical as cybersecurity.

A better case may be made for discussing cybersecurity in the context of the Conference on Disarmament. The CD has a limited membership, made up of some of the most dedicated actors. At the same time, it has invited UN Member States that have expressed a desire participate in the CD's substantive discussions, take part in its work as observers. It is true that for the past 19 years, the Conference has been unable to agree even on its work-plan. However, the CD and its predecessors have negotiated numerous major multilateral arms limitation and disarmament agreements, such as the Treaty on the Non-Proliferation of Nuclear Weapons, the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, and the Comprehensive Nuclear-Test-Ban Treaty. Once the GGE process will have run its course, it may be worth exploring whether the Conference's 65 Member States, presented with international cybersecurity as a new issue, could break their current deadlock. This, however, would require very careful preparations, including a clear definition of the Conference's mandate. We are a long way from that point!

This is best done through transparency and confidence building measures.

This can usefully be taken forward in regional organisations. Regional organisations bring together those states that are most likely to have difficult relations: It is far more likely that two neighbours share a dispute over a border area, the delineation of a sea border, or the use of natural resources than

that two far away countries are in conflict. Regional organisations provide a forum for such neighbours talk, and, ideally, to resolve their grievances.

This is especially valuable regarding cyber incidents. As mentioned before: the perpetrators of hostile cyber actions are difficult to identify. Consequently, state that falls victim to such an action in most cases has to guess who is responsible. Chances are that suspicions will fall on a neighbour with whom relations are strained. If, on the other hand, relations are relaxed and mechanisms exist to resolve any incipient disputes, the danger of escalating international tensions over hostile cyber act is greatly reduced.

In the field of cybersecurity, there is a number of concrete steps that can be agreed between members of a regional organisation. The UN Cyber GGE has sketched out a number of them.

In Europe – or rather: in the area ranging from Vancouver to Vladivostok – the OSCE has taken a leading role in efforts to reduce the risk conflict stemming from the use of information and communication technologies. The OSCE was first regional organisation to establish a working party dedicated to this end. The initial set of measures to reduce the risk of conflict stemming from the use information and communication technologies agreed by OSCE Participating States in December 2013 was first set of such measures anywhere. With these steps, the OSCE has influenced discussions in a wide range forums from East Asia to Africa and Latin America.

“ In Europe – or rather: in the area ranging from Vancouver to Vladivostok – the OSCE has taken a leading role in efforts to reduce the risk of conflict stemming from the use of information and communication technologies.

The progress made in the OSCE has strongly influenced discussions in the UN GGE, and vice versa. It is indicative that the GGE in June 2013

recommended a three-step-approach to cyber confidence building, which then was taken up in OSCE: in December 2013, OSCE Participating States agreed upon set of co-operative measures aiming at transparency building. Since last year, the OSCE working group to reduce the risk of conflict stemming from the information and communication technologies, has been discussing a second set of confidence building measures, aiming at trust building and co-operation. And in the longer term, the group hopes to arrive at third set that would be geared toward risk reduction and increasing stabilization.

The first agreement, endorsed by the OSCE Council of Ministers in December 2013, contained various voluntary steps, including:

- Providing national views on various aspects of national and transnational threats to and in the use of Information and Communication Technologies;
- Facilitating co-operation among the competent national bodies and exchanging information;
- Holding consultations in order to reduce the risks misperception, and of possible emergence of political or military tension or conflict that may stem from use of Information and Communication Technologies;
- Nominating contact points;
- Providing a list of relevant national terminology.

Implementation of these confidence building measures has begun in a serious and workmanlike fashion – irrespective of the political turbulences that have been shaking the OSCE area since late 2013.

Picking up on experiences made in the OSCE, 2015 GGE report goes into more detail concerning confidence-building measures to strengthen international peace and security and provide a peaceful ICT environment. This kind of “cross-fertilisation” is fruitful. It would be useful now for the OSCE to pick up some strands of the work done in the UN.

The 2015 GGE recommended a number of voluntary, non-binding norms of responsible State behaviour for consideration by States. It may be worth exploring how these can be translated into concrete action by the OSCE. This would not aim at regional norm-setting, but at applying universal norms in a regional context.

Here are some examples how OSCE Participating States could use norms that the GGE has proposed for confidence- and stability building.

The GGE has put forward that *“in case of ICT incidents, states should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences”*. An OSCE-agreed “check-list” of considerations and procedures could be helpful to this end.

GGE experts also recommended that States should consider “how best to co-operate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs”, and implement other co-operative measures to address such threats. Would it be useful to develop OSCE mechanisms on this? Similar questions spring to mind on how to implement the GGE recommendation that “States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts”.

It may be useful for OSCE Participating States to agree on procedures for “reporting ICT vulnerabilities and for sharing associated information on available remedies”. This is another GGE recommendation, and it seems fit very nicely with the OSCE’s interest in co-operative measures.

Some GGE recommendations should easily be agreeable to all: The UN experts found that States should *“not knowingly allow their territory to be used for internationally wrongful acts using ICTs”*. They also held that states should *“not (...) conduct or knowingly support ICT activities contrary to obligations under international law that intentionally damage critical infrastructure”* or otherwise impair the use and operation of critical infrastructure, *“should not conduct or knowingly support activity to harm the information systems of another State’s authorised emergency response teams, and should not use authorised emergency response teams to engage in malicious international activity”*. OSCE Participating States should consider publicly endorsing these norms; the proper format for such an endorsement would need to be discussed. This would increase their visibility and inspire similar action in other regions of the world.

Germany, when it assumes the OSCE Chair in 2016, will make cyber an important part of its program. We hope Participating States will support seeking some inspiration from the work of the GGE not only in the political-military dimension, but also in the economic and human dimensions of the OSCE.

This brings us to the third lesson drawn from arms control experience: Help other actors build cybersecurity capacity.

The GGE has recommended that states *“should take appropriate measures to protect their critical infrastructure from ICT threats”*. This is a matter of states’ responsibility, but there have already been suggestions to explore critical infrastructure protection under the OSCE’s economic dimension. The same applies to idea that *“states should ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products”*. This is a complex challenge; it may be necessary to involve the private sector and science community. The same is true for devising ways of *“preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions”*, as the GGE has recommended.

The GGE has dedicated an entire chapter of its report to *“International Cooperation and Assistance in ICT Security and Capacity-Building”*. This text provides a host of suggestions for concrete measures that States could undertake, such as improving the cybersecurity critical infrastructure, for instance by raising awareness of industrial control systems’ cybersecurity, and on developing crisis management procedures in case of widespread disruption of critical infrastructure service.

More needs to be done. In an unequal world where political interests vary and countries differ in their stages of digital development, it is not easy to find a consensus approach. While cyber capacity-building has become a buzzword, we are seeing relatively sparse action by digital advanced countries. This may be reason to begin through bilateral and regional initiatives – for example in the OSCE, which so far has not been active on cybersecurity capacity-building.

When we engage in Cybersecurity capacity-building, the focus must be preventive! In this sense, one

the best measures states can take is to decentralise critical systems. An electricity grid, for instance, that is locally autonomous is far more resilient than one that has a central “cyberattack node”. In a similar vein, e-government services, banking, health services etc. stand to gain in resilience from decentralised organisation.

“ Lasting security cannot be achieved without respect for human rights and functioning democratic institutions.

With regard to the human dimension, all OSCE participating States have agreed that lasting security cannot be achieved without respect for human rights and functioning democratic institutions. They have committed themselves to a comprehensive catalogue of human rights and democracy norms. In this spirit, the OSCE could usefully explore the GGE recommendation that states, “*in ensuring the secure use of ICTs, should guarantee full respect for human rights*”. This could cover OSCE-agreed fundamental human rights and freedoms, the rule of law, as well as the important work already done on Internet freedom by the OSCE Representative on Freedom of the Media. Pertinent UN General Assembly resolutions, as well as work done in the Human Rights Council and by special rapporteurs might usefully inform OSCE efforts, as well.

In a speech in the OSCE Permanent Council on 2 July 2nd, 2015, German Foreign Minister Steinmeier said that confidence is created when we face our common threats together. He pointed at risks in cyberspace as an area where we could do with more co-operation. In this spirit, and drawing on work done in the United Nations, Germany would like to explore how to deepen and widen the OSCE’s work on cybersecurity during the German chairmanship of the OSCE. ■

OPINION

THE ROLE OF THE STATE IN CREATING THE SAFE CYBERSPACE AND ITS ATTITUDE TOWARDS THE INTERNET OF THINGS



RAFAŁ MAGRYŚ

Rafał Magryś is a specialist in both designing and implementing IT systems for the public administration, and also in implementing recovery scenarios for the projects at risk. In the years 2013-2014, he was the undersecretary in the Ministry of the Interior, responsible for: preparation, production and implementation of e-services for CEPIK, PESEL modernisation, launch of CBE (Cross Border Enforcement) in Poland and datacenter modernisation for the national registry. Since 2014, he has been working in Exatel, currently as a Director of Office for Projects and Risk Management Surveillance.

In the recent years, there has been a growing technological trend, namely that of communication and co-operation between devices for the purpose of more effective, more intelligent and more precise functioning: the Internet of Things. The exchange information between the devices takes place without the participation of a man, who is exempted from the laborious collection and processing of redundant data. The trend has already included the products of large concerns such as: vehicles, production machines, small household appliances as well as effects of experiments of hobbyists based on Arduino or Raspberry Pi, to name a few. The simplicity of components allows, at a small expense, the creation of equipment for monitoring of the state of the environment, for instance: temperature, humidity, pollination or presence of poisonous gases, the construction of automatic irrigation system for your favourite polypodium or a drone, which will broadcast events from a kinder party directly to the network. Probably never before has the technology been so close to a man in the sense of a possibility of its cheap and easy use for ordinary purposes and needs.

At the same time, the always reliable Dream Factory has captured the fear of all-encompassing technology that has haunted us more or less consciously. In the latest instalment of Terminator which is entitled "Genisys", a computer network gains self-awareness and makes an attempt at taking over control of all the devices in order to implement the most dreadful of all the nightmares in the perfect world of artificial intelligence: the extermination of the redundant human race. In a blink of an eye all the devices from the Internet of Things begin to act against its own

inventors. The control of insignificant data, as it seemed, passed to the machines turns against the people; instantly we become a redundant element the technological ecosystem.

After leaving the cinema we can console ourselves with the thought of salvation brought by characters in the movie or ascertain astutely that Judgment Day regularly prophesied by Hollywood, also in the respective instalments of Terminator, somehow is still not coming. Such reactions, however, will not bring anything but the emotional comfort. They will leave us with questions about security in the cybernetic world, the limits of personal responsibility and choices, the range of responsibility of the institutions and the state. The risks which we face today also belonged to the sphere of fantasy 20 or 30 years ago. Nowadays, the use of the resources the Internet of Things, e.g. for the purpose of taking over the critical infrastructure by single persons or organised civil or military groups is as real as ever. Almost any device may be used for an attack or its preparation, and there are more and more such devices (e.g. wearables), and we often stop being aware of their presence. We are less interested here in knowing who plans a cybernetic attack and why, but rather in how to define the scope of protection and who should be responsible for it. How is the responsibility of the State to be set out? Should we treat the whole Internet of Things as the critical infrastructure of the State or should we rather rely upon the new incarnation of the "invisible hand" and count on the self-regulator? Some call for providing the unbounded freedom in the network and open access to all the resources unhindered even by market rules. Others would like to treat a citizen as person that requires

permanent care and supervision, and constitutes a threat for themselves and the institutions (which carry negative connotations particularly in our latitude).

“ Should we treat the whole Internet of Things as the critical infrastructure of the State or should we rather rely upon the new incarnation of the “invisible hand” and count on the self-regulator?

The state may not allow its resources to be attacked, and on the other hand, it is impossible and at the same time incompatible with the European system of values to introduce full control of the citizens and their ideas and activities. Therefore, it seems that actions of the State should be operationally targeted at several areas.

At the level of a citizen, it may take place through the permanent education, that is, such an education which is not limited just to schools and universities. The information about hazards must be provided by presenting and describing the risks, and also it is necessary to promote the broad knowledge about the ways of preventing and counteracting the materialisation of the risks. It is also worth thinking here about the system of organisational and perhaps even financial support for local governments and non-governmental organisations dealing with the development of digital skills as well as the appropriate complementation of the school curricula. In the process of encouraging people to use the benefits of the digital era, the message that takes into consideration the hazards inseparably related to it is rarely remembered.

It seems that the ordinary methods of education and exerting an influence may be insufficient. With the constant inundation of information the message of the State may be unheard. Therefore, just as is the case with the health care or broadly understood physical security, in order to protect the citizens, it is necessary to take advantage of “the nudge theory”¹

1 | Thaler H. Richard, Sunstein R. Cass: Nudge: Improving Decisions about Health, Wealth, and Happiness, New Heaven 2008.

focused on providing assistance in making sound choices by citizens, by expanding the area of creation of the “zero accident culture” to the area of the cyber protection.

For those who have already been attacked, it will be important to easily gain the information about the response procedures, and also the methods of giving “the first aid” to each other, and redirecting a given case to the relevant services that can provide support during the hazard.

Facing the problem of cyber protection at level of the State means, among other things, update of legal provisions. First of all, they should refer to the issue of transmission or equipment collective entities and institutions. Among other things, it is necessary to provide faster legislative response to the new emerging technologies and solutions. For instance, all too frequently, as public administration, we find ourselves in a vicious circle, which does not allow the creation of the new software adequate to the challenges faced by state institutions, as the legal provisions allowing its implementation are not ready yet.

This issue is particularly important in our country. The trend of changes related to the Internet of Things can already be observed in Poland; the intelligent devices that control the traditionally understood critical infrastructure (power, industrial and communications infrastructure) are more and more often applied in large cities. The volume of solutions and the popularity of the projects of broadly understood “smart cities” has been growing slowly.

Therefore, right from the very beginning of the road leading to the common Internet of Things, efforts must be made to secure education and influence on the activities of people in accordance with the principle that construction is usually much cheaper than reconstruction or thorough renovation. It is possible to plan the solution for three issues in the operational activities:

Firstly – in the legislative sphere – it is necessary to regard the telecommunications and ICT sector as the area that is a subject to the surveillance of the State, adequately to its significance for the

operation of the critical infrastructure of the State. The existing regulations that provide the competent minister of State Treasury with specific powers in the respective areas, e.g. power industry or mining industry must be considered insufficient in relation to the significance of communication and IT for all the processes of management of the state and the national economy,

Secondly – in the strategic sphere – the decision which analytical centre should be the leader in setting new directions and creating the strategy that determines the actions of the respective authorities. It seems that such a role should be played by the National Security Bureau (NSB), responsible for creation of security area policies not only in the civil but also in the military area.

Thirdly – the preparation of executive agendas, which, adopted by the NSB and agreed upon with the respective departments, would enter solutions into force.

There should be two such agendas in the civil area, one of them dealing with the area of building secure solutions for the State and on their basis, e-services for the citizens.

It is legitimate to use the competencies already established within the State Treasury and to transform the Central Information Technology Centre into such an agenda, a specialised unit dealing with the creation and maintenance of systems for needs of the Ministry of Interior Affairs, making it possible for the Centre to carry out tasks for whole governmental administration. The Centre constitutes an example of the strategy completed with success. It assumes that the most important systems in Poland should be carried out "in house", in order for the State to maintain full control over both: the production process and e.g. source codes. As an aside remark, let me add that the solution adopted by the Ministry of Interior Affairs has turned out to be a more financially effective solution. I am pointing here to the importance of the human resources in the government administration, responsible for the creation of the IT systems of critical significance for the State, in order to emphasise again that it is far

more effective to manage the planned construction and development of key tools using the State's own agenda than to make heroic attempts again and again at integration of the "silo" solutions which are not so much for the needs of handling specific processes concerning the citizens but rather for the needs of a specific government.

In the telecommunications department, the State needs an appropriate analytical-executive agenda. In the present geopolitical situation, the "Cybersecurity doctrine for the Republic of Poland²" published in January this year includes, among other things, the problem of the structure of ownership of the telecommunications service providers (including the transnational carriers) in the main risks. The significance of providing the effective control of the State is in my opinion the most important thing in the case of communication for the needs of the processes

“ In the telecommunications department, the State needs an appropriate analytical-executive agenda.

of State management, crisis management and the processes related to the internal security. Thus, it is necessary to build competences in the organisations remaining under the supervision of the State. For this reason, Exatel S.A., a telecommunication undertaking controlled by the State Treasury, is predestined to assume the role of the state telecommunication agenda. In fact, at present Exatel plays the role of the operator of strategic networks, providing access to the System of State Registers for thousands of municipalities in Poland, including the register of personal identification numbers (PESEL) as well as communication for the CEPIK system (Centralna Ewidencja Pojazdów i Kierowców – Eng. Central Register of Vehicles and Drivers), providing the line operation for the network that supports OST112 or communication between the locations of the Ministry of Defence. However, it is necessary

2 | National Security Bureau, Cybersecurity doctrine for the Republic of Poland, 2015 [online]. <https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf>

to allow it to act de iure, i.e. by empowerment Exatel S.A. in the system of the State, in such a way as to simplify in general the mode of entrusting the respective tasks and to indicate the areas of responsibility of the operator of the strategic networks. Perhaps the subject of operations of such an operator should also include the preparation the draft of standards related to the implementation and provision of security of the “smart city” solutions with regards to the intelligent metering, street traffic control or pressure and quality of water supplied by municipal companies.

Of course, such an agenda should not aspire to turn to the retail market and compete with other operators in this area, just like, for instance, the construction of the access networks should take place also using the existing infrastructure of other operators, if it is possible.

To sum up, it needs to be recognised that the scope of understanding of the critical infrastructure of the State must be broadened, also to include the protection of the ICT area, including the Internet Things.

The actions must be energetic, fast and not only in the sphere of strategy but also in the sphere of operational actions such as, for instance, the appointment of the aforementioned executive agendas.

Poland must brace itself – pointing to another suggestive picture from the pop culture – “winter is coming”. ■

FRAMEWORK OF UKRAINIAN NATIONAL SYSTEM OF CYBERSECURITY



PROF. OLEKSANDR V. POTII

Prof. Oleksandr V. Potii is a colonel, Doctor of Technical Science, Professor of Department of information systems and technologies security of V. N. Karazin Kharkiv National University. He graduated from the Kharkiv Higher Military School of Rocket Forces as an Engineer in Radioelectronics in 1993. In 1996, he received a Ph.D. degree in Automatic Control Systems for Armed Forces. In 2008, he was awarded a doctoral degree in Information Security Systems. He has published more than 100 articles dealing with issues of information security, cryptography, PKI and e-services. He took part in the development of national standards and legal documents related to information security, cybersecurity strategy of Ukraine and e-ID Strategy of Ukraine. He is a guest lecturer at the Kharkiv National Aerospace University and Kharkiv National University of Radioelectronics.

Tragic events have occurred in Ukraine today. Open Russian aggression is inflicted not only upon eastern Ukraine, but also add that Russia runs the information war against Ukraine. Being more precise, the aggressive propaganda of the “Russian world,” attacks on governmental information resources, slander in the media – these are all examples of violations of Ukrainian cyberspace. Consequently, these events have led to a new understanding of cybersecurity issues in Ukraine. Therefore, the President and government are taking new initiatives in the field of cybersecurity. Evolving challenges and threats made it necessary to develop a public policy in the field of cybersecurity.

The possibilities of cyberspace, the development and implementation of new information and communication technologies provide great circumstances for the accumulation and use of information, and create a fundamental dependence on their functioning in all spheres of society and the state: economy, politics, spheres of national and international securities and so on. This dependence is a vulnerable point in the operation of facilities and critical national infrastructure. On the other hand, it enables criminals to realise unlawful actions in cyberspace by destroying the integrity, availability and confidentiality of information, and damage information resources and telecommunication systems.

Towards that effect, in 2012-2013, the Parliament of Ukraine recommended amendments to some laws of Ukraine. However, the new political and economic reality demanded more comprehensive solutions from the country’s leadership. At the end of 2013 and in the beginning of 2014, a number of draft documents were elaborated that are currently under discussion.

These include: Law of Ukraine “On the basic principles to ensure cybersecurity of Ukraine,” Presidential Decree “Strategy for ensuring cybersecurity of Ukraine,” Resolution of the Cabinet of Ministers of Ukraine “On approval of the agenda for protection of state information resources from unlawful interference in their activities.”

1. The regular basis of national system of cybersecurity

Legal foundation to provide cybersecurity in Ukraine is the Ukrainian Constitution. Article 17 of the Constitution tells: “Protection of sovereignty and territorial integrity of Ukraine, provision of economic and information security are important functions of the state and the people of Ukraine.” The new National Security Strategy defines cybersecurity as a priority for the state.

Ukrainian legal framework in counteracting to crime in cyberspace only partially meets the needs of the time and does not always cover all key elements needed to effectively counter cybercrime. Today in Ukraine, there is a number of laws and other normative documents of different levels covering the problem of providing state’s cybersecurity. In particular, the Law of Ukraine “On State Service for Special Communication and Information Protection of Ukraine,” the Law of Ukraine “On information,” “On State Secrets,” “Data Protection in information and telecommunication systems” and “The National Security of Ukraine.” In addition, there are two more strategic documents: National Security Strategy of Ukraine and Information Security Doctrine of Ukraine. The Parliament of Ukraine ratified the Convention on Cybercrime. The current Criminal Code of Ukraine establishes (under Section (XVI))

responsibility for “crimes in the use of computers (PCs), systems and computer networks and telecommunications” (articles 361-363).

Today, in the conditions of internal and external aggressions, the formation of the legal framework for cybersecurity is an important task. In the recent months, the following Presidential decrees were developed: “Cybersecurity strategy of Ukraine” and “On some measures for the protection of state information resources in information and telecommunication systems,” Draft Law of Ukraine “On the basic principles to ensure cybersecurity Ukraine” and Resolution of the Cabinet of Ministers of Ukraine “On Approval of the Agenda for Protection of state information resources from unlawful interference in their activities.”

National legislation will specify^{1,2}:

- concepts and categories of cybersecurity;
- threats to cybersecurity;
- decision-making and separation of powers in cybersecurity;
- criteria for classification of objects of critical information infrastructure, formation of a list of above-mentioned objects;
- authority of government agencies to take measures to counter cyberthreats on objects of all forms of ownership;
- public and private sectors’ partnership mechanisms in providing cybersecurity.

Today, the government and the Parliament are to discuss two important documents:

- “Cybersecurity Strategy of Ukraine” which defines the basic principles of cybersecurity, the main threats to cybersecurity and the main actions of the government of cybersecurity of Ukraine.
- The Law of Ukraine “Fundamentals of Providing cybersecurity of Ukraine” which defines the national system of cybersecurity and the principles of its functioning.

The National security strategy has defined threats of cybersecurity as the main threat of national security. This way, we distinguish two basic threats from the point of view of national security. Firstly, it is the vulnerability of critical information infrastructure and state information resources. Secondly, the system of protection of state secrets and other information in Ukraine is physically and morally obsolete. The development of a national strategy for cybersecurity is caused by a sharp aggravation of these and other vulnerabilities.

“ The National security strategy has defined threats of cybersecurity as the main threat of national security.

The National Security Strategy identifies 9 priorities for cybersecurity in Ukraine. They are:

1. Development of information infrastructure of the state.
2. Creation of a cybersecurity-providing system.
3. CERT network development.
4. Monitoring cyberspace in order to detect present cyberthreats and then to neutralise them timely.
5. Protection of objects of critical infrastructure and government information resources from cyberattacks.
6. Resection of the software, including outgivings developed in Russia.
7. Reformation of the system of secret information and other undisclosed information, protection of state information resources, e-government systems, technical and cryptographic systems taking the experience NATO and EU countries into account.
8. Creation of a system of training in the field cybersecurity.
9. Development of international co-operation in the field of cybersecurity.

These priorities are defined in a separate chart of the National Security strategy and cybersecurity is an integral part of national security now. Since 2013, National Strategy for cybersecurity has developed very actively.

1 | Dubov D.V., Ozgevan M.A. Cybersecurity: the World Tendencies and Challenge for Ukraine. - K.: NISR, 2011. - 30 c.

2 | Dubov D.V. Strategic Aspects of Ukrainian cybersecurity. The Strategy Priorities, 4 (29), 2013, pp. 119-126.

2. Cybersecurity Strategy of Ukraine

Cybersecurity strategy includes five sections ^[3,4]:

- the subject area of cybersecurity which sets out the basic terms and definitions;
- identification of major threats to cybersecurity;
- defining basic principles of cybersecurity;
- defining the main directions of preventing cyberthreats;
- setting out the strategic goal of creating the National System of cybersecurity.

The strategy identifies the main challenges of cybersecurity of Ukraine under the threat of external aggression:

1. The aggression from the Russian Federation: attempts to violate the normal operation of state information resources, cyberespionage and use of cyberattacks for political purpose.
3. International cybercrime.
4. The increase of internal and external risks in realisation of cyberthreats.
5. The threats of use of information infrastructure of Ukraine as a transit ground to hide cyberattacks.

The draft strategy cybersecurity of Ukraine identified the main threats for Ukraine in cyberspace^{3,4}.

Cybercrime. Crimes using modern information and communication technologies are becoming more commonplace in the lives of Ukrainian citizens.

The new technologies are used not only for committing traditional crimes, but also to commit new crimes, especially characteristic for advanced information society. Most attention is focused on criminals who attempted violation or unauthorised use of the information and telecommunication systems of government, credit and banking, utilities, defence and industrial sectors. Classified information circulating in the information and telecommunication systems is a stable object of interest from other countries, organisations and individuals.

Cyberterrorism. Domestic enterprises, institutions and organisations, and the violation of which constitutes

threat to life and health of citizens can be a potential target for terrorist acts, including the use of modern information and communication technologies. Equally important is a threat of committing illegal acts to the detriment of third countries carried out using the information infrastructure of Ukraine.

Cyberwar. Military sector is undergoing major changes in the result of the development of cyberspace.

Most countries in the world are actively transforming their potential in defence and they are strengthening capabilities of warfare in cyberspace and protection against similar actions of the enemy as it becomes more relevant to the new types of threats. Because of the broad information security and defence sectors, defence capabilities of Ukraine become more susceptible to cyberthreats. Implementation modern information technology transforms a separate cyberspace, along with the traditional “Earth,” “Air,” “Sea” and space sphere of warfare. Appropriate level of defence capability means that there are units that are able to withstand cyberthreats defence.

The vulnerability of information infrastructure of state. Recently, information resources of financial institutions, transport and utilities, state agencies that provide security, defence and emergencies, their official websites and email servers are objects to cyberattacks and cybercrime. The sharp increase in the number of recorded cases of cyberattacks on governmental information resource affects the strengthening of hacker movement to violate the information systems of state agencies. In addition, spreads of politically motivated activity of cyberspace groups that carry out attacks on government and private websites. This leads to violations of information resources, as well as the reputation and financial losses.

The unsatisfactory state of information security which is recorded in the event of state control. This may affect the sustainable functioning of critical information infrastructure, lower the defence of the state, its economic, financial and political instability, weaken the image and attractiveness of investment and so on.

Cyber Security Strategy identifies six main threats to cybersecurity of Ukraine. They are: cybercrime,

3 | Cybersecurity strategy of Ukraine. Draft. Accessed October 15, 2014 http://www.niss.gov.ua/public/File/2013_nauk_an_rozrobku/kiberstrateg.pdf.

4 | Cybersecurity strategy of Ukraine. Draft. 2014 [online]. http://cst.org.ua/docs/lipen-O-UT/strategiya_kiberbezpeku.pdf (access: 25.10.2015).

“ Six main threats to cybersecurity of Ukraine: cybercrime, cyberterrorism, cyberwar, vulnerability of critical information infrastructure, cyberattacks on governmental resources for political reasons, unsatisfactory level of information security.

cyberterrorism, cyberwar, the vulnerability of critical information infrastructure, cyberattacks on governmental resources for political reasons and the unsatisfactory level of information security. The main objective of the Strategy is creation of modern and flexible national system of cybersecurity to protect the national interests of Ukraine in the information sphere. Our work is based on the nine principles:

1. The supremacy of law, legality and respect for the rights and freedoms.
2. Priority to the protection of personal information and citizens' rights.
3. An integrated approach to the implementation controls.
4. The priority of preventive protection measures.
5. The inevitability of punishment for the commission of cybercrime.
6. The interaction of public and private sectors in the field of cybersecurity.
7. Responsibility of critical infrastructure owners for cybersecurity.
8. The effectiveness, comprehensiveness and consistency of security controls.
9. Co-operation at the international level.

Ukraine is guided by the primacy of the citizens' rights. A very important principle is a comprehensive approach to the application of the measures and means of information protection. The relation of fight against cybercrime is confirmed by the fourth and fifth principle. We believe that the responsibility for the cybersecurity of critical

systems has to be laid on their owners, while the absolute support is provided for them by the state. The struggle against cybercrime and cyberterrorism is impossible without joint efforts of all countries. This is reflected in the ninth principle.

To sum up at this point, we consider that implementation of these principles will help to solve the main problems in the field of cybersecurity in Ukraine. The strategy identifies five main priorities until 2018. These priorities are determined by problems that already exist in Ukraine:

1. We need system of regulations that determine main cyberthreats for Ukraine. The strategy and the new law fulfil this gap. These two documents are foundation for the activities of the state and society in the field of cybersecurity.
2. National Coordinating Centre for cybersecurity is absent in Ukraine. The purpose of this centre is to coordinate Security agencies' efforts in the fight against cybercrime and cyberterrorism, as well as in the organisation of the country's cyberdefence.
3. We need to build effective interaction between government and the private sector. A large part of information infrastructure is in form of private property. According to experts, it is more than 70%. It is necessary to solve the problem of trust between government and business for effective security monitoring.
4. We must remember that Ukraine is very vulnerable in the IT sector. We widely use foreign software – about 80% of the market. Foreign hardware is almost 100%. It is necessary to build an effective system of certification and security assessment of these products.
5. Cybersecurity is the human resource. However, today we are experiencing staff shortages in specialists in cybersecurity. It should be noted that Ukraine has low culture of cybersecurity, too.

So our task is to provide cyber sovereignty of the state and build an effective system of cybersecurity. At the same time, we have to do this in a difficult economic environment and aware of Russia's open aggression.

3. Law of Ukraine “On the Fundamentals of Cybersecurity in Ukraine.”

The Law of Ukraine is the second important document of the legal foundation of cybersecurity of Ukraine^{5,6}. The law consists of three parts. Firstly, the law establishes the basic concepts in the field of cybersecurity. Next, it defines the organisational foundations of the national cybersecurity system of Ukraine. Finally, it defines the principles of international co-operation on cybersecurity. The law solves the following basic tasks:

- defines the functions and authorities of the subjects of cybersecurity;
- provides the coordination of activities of the subjects in the national cybersecurity system of Ukraine;
- creates conditions for implementation of modern approaches, forms and methods of cybersecurity;
- creates incentives to attract high-level professionals for the protection of critical information infrastructure.

The Law of Ukraine “On the basic principles to ensure cybersecurity of Ukraine” defines the basic directions of state policy in the field of cybersecurity. Creating a secure national segment of cyberspace will help to maintain an open society and to provide safe use of cyberspace by the community. An important measure in this regard is to define mandatory requirements for critical cyber information infrastructure facilities, protection of personal data, and control for the protection of information circulating on the following sites. It is necessary to develop a list of objects of critical information infrastructure which includes items that are essential to national security and defence of Ukraine. These objects require urgent protection against cyberattacks. Furthermore, it is important to provide efficient operations in regards to cybersecurity and information security units, to take effective measures to reduce the risk of threats to information and to provide security and protection of state information resources

in information, telecommunication and information, and telecommunication systems.

Improvement of public administration in the field of cybersecurity is the basis for effective preventing interference in the internal affairs of Ukraine and neutralising attacks on its information resources from other states. Strengthening Cybersecurity State will promote the development of national innovative products. It is necessary to create conditions for economic development and security of the information infrastructure of the state and its resources.

Strengthening the state's defence in cyberspace might achieve high readiness and maximum effectiveness of the Armed Forces of Ukraine in cyberspace and their ability to provide an adequate response to the real and potential cyberthreats for Ukraine. For this purpose the Armed Forces of Ukraine in conditions of cyberwarfare must be prepared – to create opportunities to reflect military aggression in cyberspace with the new challenges and threats and to protect military information infrastructure against real and potential cyberthreats. It is important to support the existing multilateral training to combat cyberattacks on public and private infrastructures, and initiate new types of exercises. This will develop a network of teams responding to computer emergencies (CERT). Another objective is to strengthen the co-ordination between defence and security sectors of Ukraine to combat cyberthreats, to strengthen technical and technological capabilities of the state and to increase scientific and human potential of public bodies responsible for the safety of cyberspace in Ukraine. There will also be a system of trainings in the field of cybersecurity for the Armed Forces of Ukraine and other security and defence sectors of Ukraine.

What are the main reasons for the failure to fight with cybercrime and cyberterrorism in Ukraine? Firstly, there are no established definitions of key terms and concepts (“cyberspace,” “cybersecurity,” “cyberattack,” “cyberwar” and “cyberterrorism”) that can be effectively applied in the practice of law enforcement. Secondly, unformed and unreformed current legal framework in the field of cybersecurity. Thirdly, lack

5 | Law of Ukraine „On the basic principles to ensure cybersecurity of Ukraine” Draft. 2013 [online]. w1.c1.rada.gov.ua/pls/. (access 04.06.2013).

6 | Law of Ukraine „On the basic principles to ensure cybersecurity of Ukraine” Draft. [online]. <http://www.dstszi.gov.ua/dstszi/control/uk/publish/article>. (access 17.09.2014).

of a unified national system against cybercrime with the relevant normative assurance.

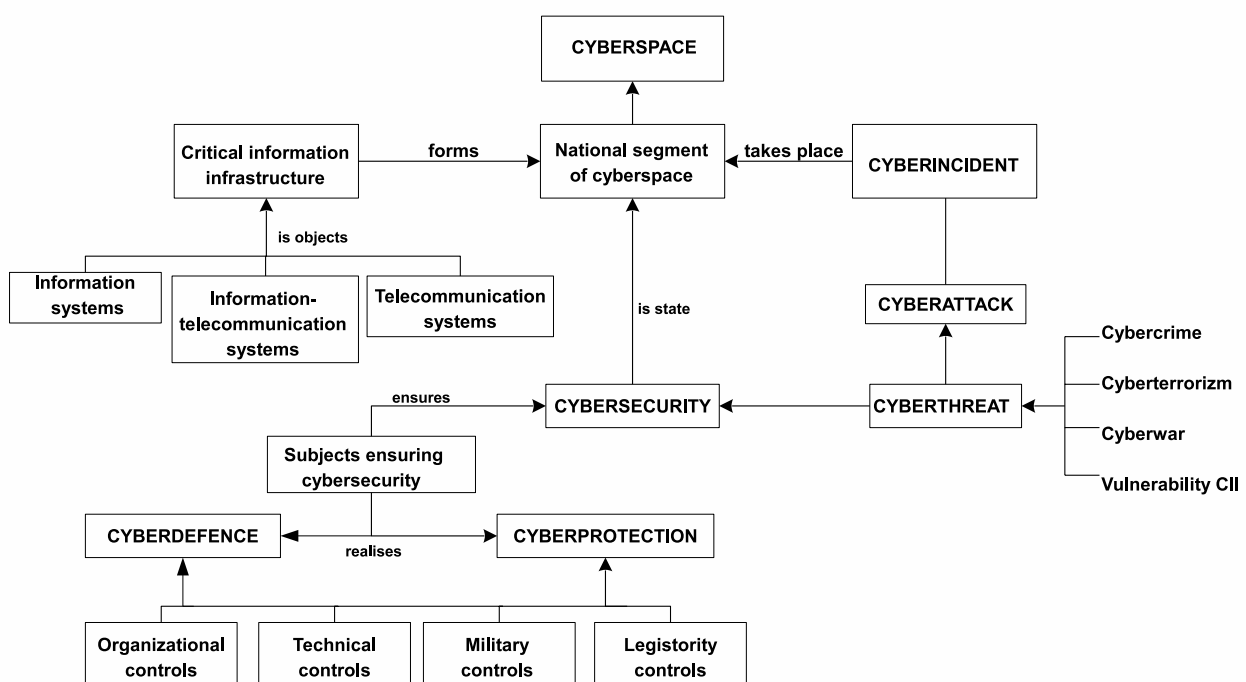
To solve these problems, it is necessary to improve the regulatory and legal frameworks in the field of cybersecurity, in particular to provide the implementation of the Convention on Cybercrime ratified by Ukraine on September 7th, 2005 №2824, in national legislation, to improve the criminal law and to allocate separate elements the crime where object of illegal encroachments are elements of critical infrastructure. It is important to carry out regular monitoring of cyberspace in order to timely detect, prevent and neutralise cyberthreats. Moreover, it is crucial to increase level of international co-operation on cybercrime and cyberterrorism in the area of cybersecurity at the national and departmental level. This will strengthen the fight against cyberterrorism and the protection of critical information infrastructure objects. This will also prevent and stop violations in the field of national security in cyberspace of Ukraine and will increase level of compliance with international obligations to fight cybercrime and cyberterrorism.

An important activity is reducing the vulnerability

of objects of critical information infrastructure. One of the main tasks in this area is to provide resistance of critical information infrastructure on incidents and unlawful acts in cyberspace. The work of management should be aimed at providing strict compliance with the heads of managing the objects critical information infrastructure, legal requirements for the protection of state information resources and cryptographic and technical protection of information, including personal data protection.

In the field of foreign activity, it is vital to provide Ukraine's full participation in the European and regional systems providing cybersecurity. It is important to enhance the role of Ukraine as active participant in the formation of global policy on cyberspace protection and on supporting international initiatives in the field of cybersecurity, taking the national interests of Ukraine into account. Government activities will focus on providing Ukraine's participation in the European and regional systems providing cybersecurity and observance the assumed international obligations in the field cybersecurity. Government activities will also promote prevention of the militarisation of cyberspace, facilitate the creation of international rules of conduct

Fig. 1. The ontological model of cybersecurity domain.



of States in cyberspace and improve the international legal framework in accordance with challenges to national and international securities.

This model describes the terminology of cybersecurity system. The central concepts here are cyberspace and cybersecurity.

Cyberspace – environment which is formed as a result of the operation of information (automated), telecommunications and information technology systems.

Cybersecurity – state of protection of life important interests of citizens, society and state in cyberspace. Critical information infrastructure forms the national segment of the cyberspace. Information and telecommunication systems are the objects of critical information infrastructure. Cybersecurity is one of the cyberspace's conditions. Cyberthreats, cyberattacks and cyberincidents are potential or real events and actions that violate the state of cybersecurity.

Cyberthreats – existing or potential events and possible factors that threaten cybersecurity

Cyberattack – unauthorised actions committed using information and telecommunication technologies and aimed at violating the confidentiality, integrity and availability of information in cyberspace.

Cyberincidents – extraordinary events associated with implementation or attempts to carry out cyberattack.

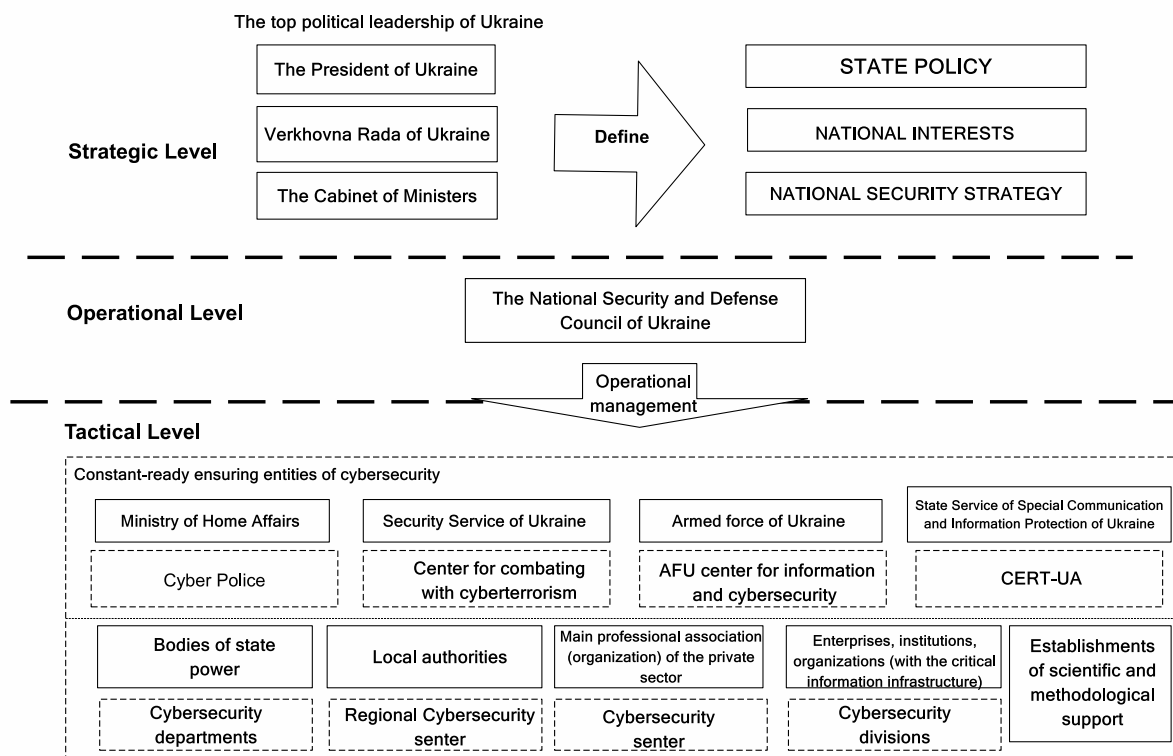
Authorised agents provide the necessary level of cybersecurity. The agents are the active elements of the national system of cybersecurity. They carry out a cyberdefence and cyberprotection of critical information infrastructure, and the national sovereignty of cyberspace.

Cyberprotection – a set of organisational, legal, military, operational, technical and other measures aimed at providing cybersecurity.

Cyberdefence – a set of political, economic, social, military, scientific, technical, informational, legal, organisational and other measures to protect the sovereignty of information and to provide the defence of the state in cyberspace.

Issues of cybersecurity need to be addressed systematically. It is necessary to take the whole range of threats, familiar sources of threats, goals and motives of cyberattacks in the national cyberspace

Fig. 2. The national cybersecurity system model.



into account. Therefore, it is necessary to establish national system of cybersecurity.

The subject of reinforcement of cybersecurity will be the core of the system. Among the subjects there are certain that need to be in a state of permanent readiness.

Cybersecurity objects are those of critical information infrastructure and other information and telecommunication systems, involving state information resources and another information.

“ Issues of cybersecurity need to be addressed systematically. (...) it is necessary to establish a national system of cybersecurity.

4. Structure of the National System of Cybersecurity

Structure of the state bodies, which are now responsible for the maintenance of information security in Ukraine is described by the author⁷.

Let us consider the structure of the national system of cybersecurity. The system has three levels: strategic, operational and tactical (fig.2).

The strategic level of management is assigned to the highest leadership of the country that is the President of Ukraine, the Verkhovna Rada of Ukraine and the Government. Senior management determines the country's national interests in the information sphere and in the field of cybersecurity. These interests are reinforced by national security strategy and the strategy of cybersecurity.

The operational level is represented by Council National Security and Defence. The Council manages the subjects of cybersecurity, it coordinates their activities and monitors cybersecurity and threat analysis.

The tactical level will form the subjects of cybersecurity. Security agencies play the key role

in this process. They are: the Ministry of Interior, Security Service, the Armed Forces of Ukraine and the State Service for Special Communications and Information Protection. These agencies form a cyberdefence system, system of fighting against cybercrime and cyberterrorism, and security of governmental information resources.

Security agencies will form the units of permanent readiness. Their tasks are constant monitoring of cybersecurity threats, rapid response to incidents of cybersecurity, suppression and investigation of cybercrime and cyberterrorism acts, and maintaining cyberdefence of the state in permanent readiness.

It is important to emphasise that Ukraine has already created practical mechanisms and units of cybersecurity. The department of state interests' protection in information sphere has been operating as a part of secret service of Ukraine since 2009.

In 2010, the Department responsible for the fight against cybercrime was formed in the Interior Ministry. On October 15th, the Minister of Internal Affairs announced the establishment of the new Police structure in Ukraine – Cyberpolice⁸. State Service of Special Communication and Information Protection has created the State Centre of cybersecurity and the CERT team^{9,10}.

Special units were created in the Armed Forces of Ukraine.

These tasks will be carried by other subjects of cybersecurity. An important role in providing cybersecurity will be given to the civil ministries, local authorities, public and private companies, as well as non-governmental and professional organisations. This will implement a comprehensive approach to cybersecurity and partnership between government and business.

8 | Ministry of the Interior. [online] <http://mvs.gov.ua/mvs/control/main/uk/publish/article/544754> (access 10.09.2014).

9 | Korneyko O. State Service of Special Communication and Information Protection of Ukraine – a key factor in the protection of public electronic information resources in Ukrainian cyberspace. Presentation of report on international conference "Cybersecurity-2013", Yalta, Ukraine. e-mail message to author, (access 02.10.2014).

10 | The main tasks of the State Service for Special Communications and Information Protection of Ukraine // State Service for Special Communications and Information Protection of Ukraine. [online] http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=89831&cat_id=89828. (access 15.09.2014).

7 | Potii, O. V., Korneyko O. V., Gorbenko Y. I. Cybersecurity in Ukraine: Problems and Perspectives. Information & Security: An International Journal. 2015, Vol 32(1) – p. 1-24.

5. Conclusion

The President of Ukraine and the government understand the contemporary challenges and threats to cybersecurity, and consider the problem of cybersecurity to be a priority of national security. Cybersecurity strategy of Ukraine has been developed. It identifies the main threats, principles and directions of the state policy on cybersecurity of Ukraine. The new law on the basics of cybersecurity forms the legal basis for building a national system of cybersecurity. The law defines the substantive scope of cybersecurity, objects and subjects of cybersecurity and the overall structure of the national system of cybersecurity. Priorities for cybersecurity Ukraine are:

1. Raise public awareness and improve the culture of cybersecurity for Ukrainian citizens. Building a culture of human security is a very important task. Citizens should be aware of the risks of using e-services. They need to know the minimum security requirements. They must be able to act in emergency situations. Public awareness of cyberthreats is an important element of the state of cybersecurity.
2. Development and implementation at the national industrial base of national cryptographic standards. Powerful industrial base systems and information protection are important elements of the national security. An important area is the development of national standardisation encryption standards. Ukraine has already developed a national standard block encryption (DSTU 7624:2014. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm) and digital signature (DSTU 7564:2014. Information technologies. Cryptographic Data Security. Hash function). We develop standards for stream encryption and hashing functions. National cryptographic standards are an element of security assurance for cryptographic security systems. National production of cryptographic protection reduces security risks.
3. Providing Security's cloud technologies. A cloud technology is widely used in business and public lives. However, they are the source of new threats for confidentiality and privacy. Security's cloud

technologies are ones of the priorities in protecting the cyberspace.

4. Harmonisation of international and European standards in the field of information security. Ukraine has clearly defined the motion vector of integration with the European Union. It is necessary to analyse the state of standardisation of the EU in the field of cybersecurity. Harmonisation of European standards is an important task. It will integrate the Ukrainian market of electronic services in Europe and will eliminate technical barriers in trade.
5. Development of a national PKI creation of a national infrastructure trust e-services. In this area it is necessary to solve a lot of problems. It is necessary to solve problems of practical use of PKI - unification, standardisation, interoperability, scalability and cryptographic strength guarantee. It is necessary to have the task of creating the infrastructure of electronic trust services. The creation of such an infrastructure should be based on national PKI. This will provide a digital signature, a digital stamp, authentication websites and electronic document delivery. The PKI system is a trusted party. It allows us to provide services to the integrity, non-repudiation and confidentiality of electronic documents. It is necessary to clarify the concept of electronic identification, analyse the state of standardisation and experience of implementing electronic identification in the EU.
6. Problems of accessibility to information about critical national infrastructure: 1) to protect against unauthorised access; 2) availability for authorised users. This service is particularly important in terms of cybersecurity. The information disseminated by Snowden, and a recent development in Ukraine show that the protections against unauthorised access and unauthorised data entry are very thoroughly monitored by security services. The technologically advanced countries allocate considerable resources for the solution of such problems. Furthermore, privacy, which is very important, is provided by the protection against unauthorised access to information and resources. ■

UP-COMING PROJECT

NATO ROAD TO **CYBER**SECURITY

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 5
- NATO cyberco-operation with the EU
- Offensive cybercapabilities
- Co-operation with the private sector

Get involved!



THE KOSCIUSZKO INSTITUTE

OPINION

CYBER TECHNOLOGIES NEW EXPERTISE OF POLISH ARMAMENTS GROUP



ARTUR KOŁOSOWSKI

Artur Kołosowski. President of the Management Board and CEO in WCBKT S.A. - one of the companies belonging to the Polish Armaments Group. Graduate of Military University of Technology, from the Faculty of Cybernetics, and Visiting Professor at this University. Leader of cyber technology domain in the Polish Armaments Group, responsible for part of a strategy in the area of cyberspace solutions. For many years associated with the Ministry of National Defence and the Polish Armed Forces. He also worked in the Office of Electronic Communications.

Cyber technologies providing safe and effective information process, storage and transmission are enormous significance for the development of strategy of all products and services provided by the Polish Armaments Group (PGZ).

PGZ is a strong and modern entity aspiring to become a key technology partner capable of competing and co-operating on global markets for Polish Armed Forces within the process of modernisation. PGZ consolidation gave the opportunity for Polish Arms Industry to benefit from technology transfer, development of cutting-edge products, creation new jobs and strengthening Group position on the international markets. It is also a chance to establish long-term co-operation with the largest and the most technologically advanced companies of the defence sector.

Improvement through domains

All the companies under PGZ umbrella have strong, leading position in the area of their activity. Apart from development in the existing competencies, the strategy for 2015-2030 focuses on selected, most promising areas, both technology and commercial. The Group objectives correspond with the program of Polish Military modernisation and are indicated as "product domains" for the PGZ strategy purposes. The strategies of product domains are intended make the best possible use of manufacturing and engineering potential and expertise research and development resources offered by organisational units. Such approach allows to identify and enhance the synergy, it also underlines the need for mergers and acquisitions, and sets new directions of co-

operation with business partners. In addition, the product domains will embrace system solutions, which will allow the Polish Armed Forces to take the most ambitious modernisation challenges in close co-operation with the sector of Polish defence companies.

Product domains include, in particular, ground platforms, sea platforms, anti-aircraft defence, air platforms, ballistic weapons and defence, electronics and information technology, ammunition and rocket missiles as well as rocket artillery. Cyber technologies as well as aerospace and satellite technologies have been already developed in Poland and obviously implemented in PGZ products. However, due to their importance they have been defined as separate product domains.

PGZ potential will be tapped for preparing solutions to provide information and communication security in the military and business. The structure of digital infrastructure, based primarily on the internet, is being continually enhanced and developed what provides PGZ with new business opportunities related security in the cyberspace.

Cybersecurity in the Republic of Poland

When planning the future development of PGZ capabilities in the field of cyber technologies, the formal aspects of this area shall be taken into account, above all the Doctrine of Cybersecurity of the Republic of Poland as a cross-sectoral administrative document for the National Security Strategy.

The recommendations of the Doctrine of Cybersecurity

of the Republic of Poland are addressed to all state-owned and private-owned entities involved into planning, organising and executing cybersecurity aspects. PGZ intends to be an active participant of the cybersecurity debate and the expertise centre within this area.

When planning the development of technologies and engineering solutions intended for information processing, assumed that cybersecurity goes beyond strictly engineering activities and embraces numerous complex processes connected with security. The specificity of contemporary threats is radically different from those characterising conventional conflicts. Thus, the rules of conduct have to be adjusted to the changing reality. We take that into account while arranging the use of information and communication solutions integrate command, control, and reconnaissance, and target guidance systems. Field management of broadly understood cyberspace conflict has become one the major components of Poland's defence policy.

PGZ's experience in designing military solutions can be also applied in civil sectors of the economy. Protection of Polish critical infrastructure against cyberthreats can be an example of the Group's concern. Cyber protection of critical infrastructure facilities is indispensable for the continuous operation of the economy and security the citizens. It is also vital for the efficient operation national security management subsystem, defence and protection of subsystems as well as economic and social support of subsystems.

Security and immunity

Entities in the PGZ Group have remarkable potential in the field of development, design and manufacture of electronic devices and software, including systems providing protection and processing of classified information. The majority of companies are also experienced in using or building devices related to electromagnetic security. PGZ companies offer includes products and services within the area of cybersecurity. These are, in particular, critical infrastructure protection, alarm, spatial observation, classified information processing systems and

electromagnetic immunity tests.

The most important assets of PGZ are extensive research and development capabilities and ability of performing complex implementations in the environment characterised by highest quality and security demands. Entities belonging to PGZ have well trained and qualified staff consisting of designers, electronic engineers, IT specialists, mechanics and process engineers. Employees can participate in projects for the new technologically advanced electronic devices, software and applications customised to the needs of most demanding users.

System approach to new cybersecurity projects embraces, among others, process algorithmisation and building the capability of merging distinct information systems. The capacity to build new experiences results also from the practical skill project execution in co-operation with global ICT defence industry leaders.

New skills

PGZ intends to build capabilities of integrating smart information networks and systems with enhanced requirements for infrastructure immunity and cybersecurity. Such smart networks and systems are characterised by autonomy and are also capable self-organisation, adaptation and decision-making, error- and fault-tolerant, scalable and predictable as regards service quality assurance, characterised by open architecture and ICT security.

As part of development of the cyber technologies domain, PGZ intends to build the capability of participating in the governmental National Smart Specialisations programme, in particular, related smart geo-information networks and technologies as well as smart creative technologies connected with smart methods of accessing to the content published in the network.

Furthermore, PGZ is going to develop its capacities related to provision of secure technological solutions as part of the National Programme for

Critical Infrastructure Protection, in its modern broad meaning, taking mutual cross-sectoral interactions and increased risk of serious and large-scale failures into account. It is necessary to offer the solutions which allow proper understanding critical infrastructure as a mutual and operatively interconnected systems – real and cybernetic. The systems are composed of facilities, devices and installations.

High-speed, large-capacity internet links – broadband networks, in fact, available to everyone, omnipresent communications, networks in enterprises and hypermarkets, schools and university webs, systems which protect state administration and military services make us linked like never before. Information is available immediately, however, the question arises – is the information availability safe? The conclusion that relevant expertise in the field broadly interpreted cybersecurity will be of long term value suggests itself.

For the Polish Armaments Group the issues related to cybersecurity is the opportunity that has to be used. ■

OPINION

EUROPEAN CYBERSECURITY MUST BE STRENGTHENED



PROF. JARNO LIMNÉLL

Prof. Jarno Limnéll 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 for 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.

European Cybersecurity Forum, CYBERSEC, was a success. It was great to meet cybersecurity experts from so many countries, discussions were both topical and interesting, and arrangements worked perfectly. A warm thank to the organisers and colleagues. We'll see again next year!

Cybersecurity has entered the domain of foreign and security policy due to the ever-globalising world. In this digital domain, strategic advantage can be either lost or won. It is very significant to encourage us Europeans to think over cybersecurity issues together especially from the strategic point of view. We are no longer securing computers – we are securing societies and our way of life. We are also protecting our values. As it says in the EU Cyber Security Strategy, *"The EU's core values apply as much in the digital as in the physical world."*

Most European countries have cyber strategies on paper, but public discussion at policy and doctrinal levels and practical measures are not as mature as they are for example in the United States. Without serious efforts in Europe the gap is only likely to widen. This would increase the potential for Europe to become the focal point for more serious cybercrime, espionage and even debilitating attacks.

But it is not easy to deal with 28 countries and despite these steps at the EU level, European cybersecurity remains almost exclusively a national prerogative. This must be changed. The most important driving force for a new "Cyber Europe" could be European industry. At the moment companies outside of Europe are dominating the rapidly growing cybersecurity market. For example, in the latest list of "cybersecurity companies to watch in 2015" there are few European companies in Top 100.

At the moment there is a special opportunity for European companies because there is a lot of suspicion in the market towards cybersecurity products from the US, China, and Russia. European companies would be able to enter the market as a more trustworthy partner.

Europeans are very dependent on foreign internet services, especially GAFA, which stands for Google-Apple-Facebook-Amazon. Nine out of ten Internet searches in Europe use Google. Where are European alternatives, many people ask? It is a very relevant question. This dominance should worry Europe, even if the current situation works fairly well.

In the US, Google, Apple, Facebook, and Amazon are generally praised as examples of innovation and the same kind of innovativeness must be encouraged and supported in Europe. The question is not only how much Google, Apple, Facebook, and Amazon dominate every facet of our lives, but also how important and precious is the data they possess in today's world. This data should be understood as a part of cyber power - and Europeans are letting it go abroad.

European cybersecurity companies and digital platform industries must transform themselves and become more competitive. This development has to be supported strongly. It is also the job of politicians and lawmakers to protect both European industries and European digital rights. Cybersecurity issues should be brought more actively into the political discussions in European governments and Europe must clearly outline its own policy – and practical activities – on topical cybersecurity questions. We have to understand that without European cybersecurity industry there will not be credible European cybersecurity. This is the only way to secure European cyber future. ■



CYBERSEC

EUROPEAN
CYBER SECURITY
FORUM



CYBERSEC

EUROPEAN
CYBER SECURITY
FORUM



ANALYSIS

EDUCATION AS A KEY FACTOR IN THE PROCESS OF BUILDING CYBERSECURITY



IZABELA ALBRYCHT

Izabela Albrycht is a Chairperson of the Board of the Kosciuszko Institute and the Chair of the CYBERSEC Organising Committee – annual public policy conference devoted to the strategic issues of cybersecurity. She is an author and co-author of publications focused on issues connected with international relations and EU Policies. She organises and co-organises research projects and conferences in Poland and abroad. She is the Editor Associate of the European Cybersecurity Journal and former Editor of the International Shale Gas & Oil Journal (2013-2014).

Over the last few decades, we moved a significant part of our multidimensional activities to the cyberspace. Aside from the obvious benefits, this process poses a huge risk for the entire civilization. The number of hacker attacks, implementations of information systems, as well as risks associated with the operation of cyberworld is rapidly increasing. In building cybersecurity we cannot sacrifice the benefits of digital, crosslinked and automatised reality. We need to catch up with “the bad guys.” To do so, we dramatically need cybersecurity specialists. This need is reflecting in growing demand for cyber talents – highly qualified cyber personnel who will be able to respond to the increasingly sophisticated forms of cyberattacks (cybersecurity IT specialists) and who will be responsible for creating the architecture of cybersecurity (i.a. lawyers, political scientists, administration employees). Therefore, the key factor in the process of providing cybersecurity in public and private sectors is to adapt the education system this

new long-term challenges as well as to the market needs to educate more and more cyberspecialists. It is not possible today to fill the ever-growing gap in employment in the ICT sector, neither the education of specialists who would be responsible for adapting the legislation and institutions of state in cybersecurity or for building international co-operation in this area.

The cyber talents' gap

There is a need for IT security specialists everywhere. Without them companies expose themselves to a multimillion loss, arising from incidents on the network. This high demand for cyber talents also occurs in companies in the critical infrastructure sector, banks, defence, professional service centres and automated industries and manufacturing (Table 1). It is a particularly important issue as cyberattacks on critical infrastructure facilities endanger national security and can be elements of both the classic and the hybrid form of war.

Table 1. Cybersecurity Demand Grows by Industry Sectors

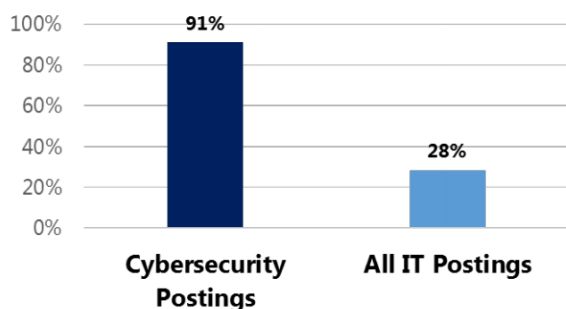
Industry Sector	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)	2010 - 2014 Posting Growth
Professional Services	37%	49,765	57%
Finance and Insurance	13%	17,873	131%
Manufacturing & Defense*	12%	15,968	57%
Public Administration	7%	9,725	N/A**
Information	6%	8,522	65%
Health Care and Social Assistance	6%	7,915	118%
Retail Trade	3%	3,505	120%
Other	15%	19,983	N/A**

Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

The shortage of IT workers for example in Poland is very high and is up to 40 thousand people. In the entire European Union – according to the data published by the European Commission – the demand for professional ICT workers in the IT sector across many sectors in Europe is growing at a rate of approx. 3% annually despite the crisis¹ while the number vacancies for computer scientists can currently reach up to 300 thousand, and it could be up to 825,000 unfilled vacancies for ICT professionals by 2020². In order meet this challenge the European Commission is leading a multi-stakeholder partnership, the Grand Coalition for Digital Jobs, aimed at tackling the lack of digital skills in Europe and the thousands of unfilled ICT-related vacancies across all industry sectors. The subject of digital skills gaps was discussed by Member States not later than December 11th by the EU ministers. According to the press release their objective is prepare the ground for a joint commitment to develop adequate levels of digital skills in the EU in the face rapid digitisation. In 2016, the Commission will present a comprehensive skills agenda³.

According to Symantec, which is one of the chief market leaders, until 2019, the demand for specialists in cybersecurity could rise to approx. 6 million people worldwide⁴. This number includes 1.5 million new posts to be created within the next three years. This tendency is also confirmed in a recent report of another huge IT company, Cisco.⁵

Table 2. Growth in Job Postings.



Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

1 | Working Paper: Digital Economy - Facts & Figures, European Commission, p. 3 [online] http://ec.europa.eu/taxation_customs/resources/documents/taxation/gen_info/good_governance_matters/digital/2014-03-13_fact_figures.pdf (access: 10.12.2015).

2 | European Commission, [online] <http://ec.europa.eu/digital-agenda/en/grand-coalition-digital-jobs#Article> (access: 20.12.2015).

“ The shortage of IT workers for example in Poland is very high and is up to 40 thousand people.

In turn, according to the report “Job Market Intelligence: Cyber Security Jobs, 2015,”⁶ last year, 238 thousand job advertisements appeared in the US related to cybersecurity. In this field, positions for professionals make up 11% of all jobs in IT sector in the United States. Since the supply is not keeping pace with the demand (in 2010-2014 the employment of cybersecurity professionals has increased by as much as 91%!), wages are higher by an average of 9 % than in the entire industry (Table 2, Table 3).

It is not just a temporary trend. This is a long-term change, which requires wise strategy and the adjustment of the educational and training system offerings.

The best examples

Nothing proves better in addressing this challenge as cybersecurity education hubs and cybersecurity centres of excellences. Lately, there is no better example of this type of initiative than Advanced Technology Park on the campus of Ben-Gurion University in Beer Sheva in Israel. Which even aspires for the title of the New Silicon Valley - place, where technologies are mainly developed just in the field of cybersecurity. We introduce something that can be called an economic anchor, which will change Beer Sheva into a national and international centre of cybernetics and cybersecurity – said in September 2013 Israeli Prime Minister Benjamin Netanyahu, opening the first stage of this investment.








3 | Commission and EU ministers discuss digital skills and review of EU telecoms rules, [online] <http://ec.europa.eu/digital-agenda/en/news/commission-and-eu-ministers-discuss-digital-skills-and-review-eu-telecoms-rules> (access: 20.12.2015).

4 | Growing cyberthreat means more jobs in US, [online] <http://www.cnbc.com/2015/08/06/growing-cyberthreat-means-more-jobs-in-us.html>(access: 20.12.2015).

5 | 2014 Annual Security Report, [online] http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf (access: 20.12.2015).

6 | Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies, 2015, p. 3 [online] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf (access: 10.12.2015).

Table 3. The Cybersecurity Workforce Overview

Title	% of Cybersecurity Postings	Number of Cybersecurity Postings (2014)
Engineer (e.g. Security Engineer, Information Assurance Engineer)	26%	42,355 
Manager/Admin (e.g. Data Security Administrator, Information Security Manager)	19%	30,586 
Analyst (e.g. IT Security Analyst, Cyber Intelligence Analyst)	18%	28,853 
Specialist/Technician (e.g. IT Security Specialist, Infosec Technician)	10%	15,289 
Architect (e.g. Security and Privacy Architect, Network Security Architect)	5%	8,409 
Auditor (e.g. IT Auditor)	5%	7,533 
Consultant (e.g. Network Security Consultant, Infrastructure Security Consultant)	4%	6,294 

Source: Job Market Intelligence: Cybersecurity Jobs, Burning Glass Technologies

After two years, we can say: in essence – it is essentially changing. And a human capital in this venture is at least as equally important as it is in financial terms.

Cybersecurity – both within domestic and international dimensions - is one of the main priorities of the Obama administration's security policy. In practice, it is also reflected in the adaptation of education system to address the sector's needs, developed together with close co-operation of commercial enterprises, government agencies (such as the National Security Agency, the Department of Homeland Security and the National Science Foundation) and universities.

In recent years, the US created numerous education hubs, regional centres of excellence specialising in cybersecurity, and national centres, such as the National Initiative for Cybersecurity Education at the National Institute for Standards and Technology. A strategy for workforce development has been established for the cybersecurity sector (National Cybersecurity Workforce Framework). A special emphasis is placed on the so-called STEM (which stands for Science, Technology, Engineering, Mathematics) in education. All of this together adds up to the national strategy of win-win, whereby particular cities and states are becoming important centres

in the field of cyberspace education. As a result of the development in information technology, many academic centres are gaining significant comparative advantages in attracting investments of the cybersecurity industry.

Since 2011 the United Kingdom government within the National Cyber Security Programme has invested in establishing training providers and a network cyber education specialists. According "Strategic Defense and Security Review"⁷ outlining the national defence strategy for the next five years, UK will speed this process up, providing targeted training for cybersecurity specialists. The schools programme to identify and encourage talent among 14-17-year-olds will be created across the UK, as well as new cybersecurity apprenticeships focused on particular sectors will be granted. UK is going to scale up existing successful programmes, including the Cyber Security Challenge and GCHQ's 'Cyber First' undergraduate sponsorship scheme. Another £20 million will be allocated to launch a new Institute Coding, which aim is to develop digital and computer science skills. Across the county in leading UK universities Centres of Excellences in Cyber Security Research have being established. The UK is also

7 | Strategic Defense and Security Review, p. 79 [online] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (access: 18.12.2015).

encouraging young people to study engineering and science. All these initiatives are providing the UK with professionals with the right cyber skills for public and private sectors. Education is perceived by the UK government as a requirement to remain a world leader in cybersecurity.

We are not prepared yet

Most of the European countries are not systemically prepared to face cyberthreats and challenges, and its education systems have not kept pace with the market needs. This state of affairs threatens the internal, international and economic security. European decision-makers need to be aware of these threats and need to increase expenditures on education, and also solutions aimed at adjusting educational offerings should be adopted to be able to tackle challenges and to provide cybersecurity of the state, public institutions and business. It is essential to support the academic centres which serve as recruitment base for the broadly cybersecurity sector. This sector should become one of the priority areas research, as it has been announced by the European Commission on December 18th, at the beginning of the public consultations on the areas of work the future cybersecurity contractual public-private partnership. The Commission stated that “the PPP will be a contractual arrangement between the Commission and an industrial grouping, both of which are committed to supporting, in the EU’s Horizon 2020 programme, research and innovation activities of strategic importance to the Union’s competitiveness in the field of cybersecurity. A PPP bringing together industrial and public resources would focus on innovation following a jointly-agreed strategic research and innovation roadmap. It would make the best possible use of available funds through better coordination with member states and a narrower focus on a small number of technical priorities. It should leverage funding from Horizon 2020 to deliver both technological innovation and societal benefits for users of technologies (citizens, SMEs, critical infrastructure), as well as provide

8 | Public consultation on the public-private partnership on cybersecurity and possible accompanying measures, [online] <http://ec.europa.eu/digital-agenda/en/news/consultation-public-private-partnership-cybersecurity> (access: 18.12.2015).

“ Most of the European countries are not systemically prepared to face cyberthreats and challenges, and its education systems have not kept pace with the market needs.

visibility to European R&I excellence in cyber security and digital privacy.”⁸

A chance (not only) for Poland

According to European Commission, there is a room for improvement in terms of educating and employing ICT specialists in Poland. “With regard to the share ICT specialists as a percentage of employed individuals Poland ranks only 21st of all EU Member States. Even though Poland has more STEM (science, technology and mathematics) graduates than most countries in Europe, it does not yet manage to use this advantage in order to increase its share of ICT specialists.”⁹ For years, Poland has been famous for its information technology talents. Nothing is missing in the quality of academic centres, which have the potential to create cybersecurity related education offerings (including Warsaw, Wroclaw and Krakow). As the analysis of the Polish Information and Foreign Investment Agency shows, these cities have a variety of educational offerings providing a large number of young, well-educated computer scientists, programmers, network administrators, system analysts, security system engineers etc. These are particularly attractive places for IT industry investment. The cybersecurity sector is a “knowledge-absorbing” sector, further characterised by good dynamics of development and innovation, therefore it is a good investment for the future.

Thus, the regions which will support academic institutions in the development of computer science, especially related to the topic of cybersecurity, can become major national centres of education: “our Silicon Valleys” – supporting the security building measurements within the Polish cyberspace. Issues related to

9 | European Commission, Poland, [online] <https://ec.europa.eu/digital-agenda/en/scoreboard/poland> (access: 20.12.2015).

cybersecurity should not be restricted to strictly technical dimensions and to information technology because what happens in cyberspace increasingly makes an impact on public policies and legislation and it is an area of conflict and a matter of international relations. It is essential to upgrade the education offerings with a “cyber” component, such as political science, international relations, national security studies, public administration and law (both on master’s and postgraduate level). Of course, the above-mentioned areas are not exclusive, but merely identify the most current needs.

Due to its competitive advantages, the most serious candidate for the city that could become a regional centre of education in Poland and in Central Eastern Europe, within the area of cybersecurity is Kraków.

Today, the biggest Polish and global IT companies (such as Comarch, Cisco, IBM, Samsung) invest in this city as well as in the entire Malopolska Region, and also the largest number of start-ups related to technology is being created. In addition, the outsourcing industry employs huge number of employees (about 40 thousand) who are extremely vulnerable to cyberthreats. In the near future, further development in the Małopolska province may be also conditional upon the accessibility to network security specialists.

Krakow is currently the second academic centre in Poland, in terms of number of graduates in information technology (very slightly inferior to Warsaw). The city is also a hub of academic disciplines as humanities, within which experts and professionals can be trained and educated, and whose knowledge and skills can be utilised to build a solid foundation for the country’s cybersecurity.

In Kraków, the biggest annual public conference in this part of the continent - the European Cybersecurity Forum - CYBERSEC was held, co-organised by the City of Kraków. This annual conference brings together specialists in this field and is a place to develop practical measures which are aimed at increasing cybersecurity within the Member States of the EU and NATO. It is a platform for community building, both for Polish and international experts, academics and professionals specialising in cybersecurity (understood as a challenge for state institutions, international organisations, business and military as well).

All of this potential can be used to create National Digital Staff Resources and contribute to the country’s security growth and to the development of the city itself.

It is also in the interest of not only the local authorities, but also of companies from the IT sector which are investing in the Małopolska province to stimulate universities in Krakow to educate more experts in the field of cybersecurity and to create a new “cyber-specialisation,” thereby extending the scope of the educational offer. It is also important for the universities to realise that there is a real demand in the business and other sectors for “cybertalents.” A push from the youth can be an important factor in this process – students should be aware that there is a “cybernetic employment gap” and by filling it, it provides career perspectives and guarantees a higher remuneration. This creates also a possibility to work in the field of national and/or economic security of the state. In this sense, it can be seen attractive for the youth, not only for financial reasons. This process requires the identification of all stakeholders, the creation of a platform for co-operation between them and the implementation of solutions which are strengthening this co-operation.

“ One of the most important challenges for the new government, including the Ministries of Digitisation, (...), is to provide a personnel with valuable skills and knowledge for our increasingly innovative and digital economy.

One of the most important challenges for the new government, including the Ministries of Digitisation, Science, Higher Education and Development in particular, is to provide a personnel with valuable skills and knowledge for our increasingly innovative and digital economy. Shifting the centre of gravity in the educational system of modern human resources in Poland has to, however, take place not only in just one city (Krakow), but also in the entire country. In the following years, we need to build together a competent “cybernation.” ■



*The next wave of the
Internet favours the brave.
We're ready. Are you?*

cisco.pl



ANALYSIS

HOW SHOULD PRIVATE COMPANIES DEAL WITH CYBERSECURITY?



AGNIESZKA WIERCIŃSKA-KRUŻEWSKA

Agnieszka Wiercińska-Krużewska - LL.M. – advocate, senior partner at WKB Wierciński, Kwieciński, Baer. Head of the intellectual property and TMT team, also closely co-operates with the M&A team. She advises clients on all aspects of copyrights, industrial property, consumer law, unfair competition, preservation of confidentiality, privacy and personal data protection, internet domains, press law and protection of personal rights. She also deals with the cases regarding critical infrastructure protection as well as the regulations on the transfer of military and dual-use technologies. Agnieszka represents clients in litigation and arbitration proceedings and she has also extensive experience in the acquisition of companies on the private market. WKB Wierciński, Kwieciński, Baehr is a leading Polish law firm, providing top-tier end-to-end legal services in key areas of business law. For more details please visit www.wkb.com.pl.

Many people wonder what “cybersecurity” means exactly and whether it is applicable to private entities. This is mainly due to the fact that cybersecurity is mostly discussed in the context of terrorist attacks, state security or the functioning of critical infrastructure. Cybersecurity is rarely discussed in relation to small or medium sized companies. As result, some people expect that safeguards should be provided at the state (or European) level rather than at the level of businesses enterprises. According to PWC report [Secured Information – Secured Future – The Global State of Information Security – December 2014¹], the number of cybersecurity incidents against private companies rises every year by around 25%. The authors of the report claim that it is almost certain that each company will have encountered an IT security attack, but some may still not be aware that it even happened.

In the early days of interconnected computers, most attacks were done for fun or the notoriety of hackers. These days, attacks are often done for money or political reasons. Currently, the global economy loses up to 550 billion dollars due to cyberattacks annually. High profile examples include: “Stuxnet” – where more than 16,000 computers of Siemens were infected with a virus that allowed to download information (2010); and “LulzSec” – where the data of more than one million Sony Playstation users was obtained. The specialised firms that make attacks to check the IT security of firms in Poland say that only 10% of tested firms are able to discover and isolate an attack.

1 | Global Cybersecurity Index & Cyberwellness Profiles [online.] <https://www.itu.int/pub/D-STR-SECU-2015> (access: 17.11.2015).



Good cybersecurity practices

1. Employers – Employee Relationship
2. Identifying Protected Assets
3. Internal Policies And Written Code Of Conducts
4. Bilateral Agreements With Employees
5. Training
6. Monitoring Software
7. Specific Incidents Response Procedure
8. Consequences

So what is a cyberattack? A cyberattack is an attack initiated from a computer against a website, computer system or individual computer (in this article, collectively, a “computer”) that compromises the confidentiality, integrity or availability of the computer or information stored on it. An attack can stop business for a while or, in some cases, forever.

Nowadays, almost every enterprise is connected to the Internet, sells through the Internet, or stores data in the cloud or on servers located outside of its place of operation, or does business with or otherwise relies on other businesses which do. Consequently, virtually every business is exposed to some sort threat connected with operating in cyberspace i.e. the networks among computers.

The respondents to the PWC survey discussed in the report indicate that the greatest risks for business are: an adverse impact on its reputation and the value its brand, the theft of IP rights (such as reports, data or plans), the theft of personal data (e.g. the data employees or customers), and internal administrative failures of its systems.

Most available information shows that companies in Poland are not prepared for cyberattacks. Moreover, not only cannot they stop an attack, but they often cannot even detect that it happened. In many cases, cybersecurity is the domain of IT departments (often outsourced) which are far from the core business of the company and do not understand the company's most valuable assets and risks. Further, few firms incorporate cybersecurity as an element of their business strategy.

There are various things that can be done by company to prevent or limit cybersecurity events and their consequences. A lot of companies, especially in the recent months, have increased their level security by introducing complex IT solutions to monitor and prevent network failures and data breaches. Such investments in security systems seem to be unavoidable. But such investments cannot be the sole approach to the issue.

Many IT experts say that even the most sophisticated firewalls will not protect companies against their weakest links – human beings, especially employees or ex-employees.

“ Many IT experts say that even the most sophisticated firewalls will not protect companies against their weakest links – human beings, especially employees or ex-employees.

So, what else can be done? The answer is not necessarily to throw more money at the IT security systems or improve the training of the IT staff or external provider. In many cases, the IT system and staff are adequate. Rather, the vulnerability might arise principally through organisational reasons. For example:

- Employees may not truly understand the key assets of the company and, consequently, they might not know what needs to be protected.
- Employees may be careless and not pay enough attention to the assets to which they have access;
- Employees may not be properly trained and have inadequate access to clearly defined policies on how to deal with valuable assets and the devices on which such assets are stored;
- The company may not have compliance programs, internal policies and staff contracts which clearly cover cybersecurity events;
- Similarly, the contracts with commercial partners quite likely do not mention issues relating to cybersecurity;
- The company might not have insured against cyberattacks, despite such insurance being readily available;
- The company may have no risk management policies on how to react if an IT security breach occurs.

From the legal point of view, while compliance programs in this area are increasingly popular, they still are not especially common. The absence such programs often leads to the failure to prepare internal policies regarding security or, even if prepared, the failure to routinely revise and update them or communicate, or remind staff about them. Also, staff contracts are surprisingly vague on this topic. Often even key personnel have no confidentiality undertakings, no competition clauses or no clearly defined responsibilities as far as access to information is concerned.

Therefore, it is crucial to introduce good practices in the field of cybersecurity, that is:

1. Employers – employee relationship

Cybersecurity events caused unintentionally by employees can be effectively limited by building strong relationship between employees and employers, based on the employees' loyalty and awareness of the risks and consequences of breaches. The best results are achieved if employees associate themselves with the employer and treat the valuable assets as if they were

their own. On the flip side, some severe security events are caused by unhappy employees or ex-employees.

2. Identifying protected assets

Before starting work on the legal framework for mitigating cybersecurity risks, the company has to define (map) its key information assets. These can include confidential information such as customer lists, pricing policies, strategic plans, designs, etc., as well as communications with business partners, and personal data kept and processed by the firm. The organisation has to be able to ascertain where the valuable information of the company lies, who has access to it and, finally, what part of this information is stored in the cyberspace. Once the key assets have been identified, in most cases, the number of employees who have to have access may be limited. For this purpose, it is important to categorise employees according to their requirements for access. The exercise should be conducted on different levels of the company and should involve as many of the personnel as possible.

3. Internal policies and written code of conducts

Critically, employees have to also be made aware what they are required to protect and why. They also have to understand, familiarise themselves with and respect policies which often involve consuming procedures. However, assuming that people in the organisation understand the importance of cybersecurity, they will generally follow and comply with policies in this respect. The implementation of the policies has to be strict and non-compliance should be a subject to disciplinary penalties, termination of employment contracts or even liability for compensation.

Many companies provide employees with equipment such as a company computer or mobile phone. Moreover, some businesses allow employees to use their private devices for business purposes. In either case, not just the employer, but also the employees may be exposed to cyberattacks and may easily become victims of cyber events. For example, it is common that attacks are made by sending emails employees that links or attachments for the purpose of gaining companies' trade secrets or infecting companies' devices with unsafe software. Moreover,

companies should be aware that despite the numerous advantages of providing employees with mobile devices, such practice exposes them to risks connected with loss or theft of the device which may result in unwanted disclosure of important information including trade secrets. A company's data may also be threatened by the unintended activities of employees on the Internet e.g. downloading data and saving it on mobile devices, or downloading software on the company's devices without appropriate permission. Additionally, the increased activity of employees on social media should also be taken into account. Cyberattacks are sometimes based on guesswork in respect of passwords which may be words commonly used by employees in social media.

These are just some of the reasons for implementing robust security policies, with special attention to the IT security policy and the data safety policy. Generally, the implementation of such policies does not require substantial financial resources, but the value may be significant.

An IT security policy has to be prepared on a case by case basis. Samples of such documents can be found on the Internet, but these should be used with caution because they are unlikely to apply to the specific circumstances of a given business.

The internal IT documents usually have one of the three forms: a policy (a binding document that is usually incorporated into the terms of employment), workplace standards or guidelines (each being documents that describe certain technical procedures or suggest certain behaviours). The IT security policy should have the form of a binding document that is approved and announced by the governing body of a company rather than being a mere guideline issued by the IT department. The IT security policy has to be easy to read and understand, and has to be adapted to the organisation in terms of subject matter, the IT system used, the size of the company, etc. The terms of the policy should be enforceable and should stipulate requirements on a "do it" / "don't do it" basis. Before being announced, the document should be broadly discussed and subject to comment. The staff of an organisation are often the best critics and may have valuable suggestions. All policies should spell out

consequences for non-compliance. However, in order to take account of the variety of situations in which breaches may occur, the employer should always reserve the right not to impose them against a violating employee. Furthermore, each organisation still has to focus on doing its core business. For that reason, each and every policy has to be reasonable and should avoid imposing onerous limitations in a blanket manner when such requirements are only applicable to extreme situations.

What are the main areas that the employer should focus on in the policy?

Use of private equipment: In the event that employees use their private equipment for business purposes, there should be a policy covering such arrangements. The policy should allow the use of personal devices for business purposes only under certain conditions e.g. only if such device is protected by special programs which effectively detect and remove viruses. In some companies, especially where trade secrets require strong protection, it is justified to prohibit the use of private devices for business purposes.

Use of the company's equipment for private purposes: Due to the common availability of IT devices, the use of company's equipment for private use is less frequent than a couple of years ago. Still, it constitutes a major risk to IT security. Some basic restrictions should be imposed such as prohibition on using the same logins and passwords as for privately used devices, a prohibition on providing a company email address to privately used services, a prohibition on making a company device accessible to third persons, and a prohibition on visiting certain types of risky websites on Internet. The employees should also be made aware which programs can be installed and kept on their company devices. Moreover, they should be instructed about spam filters and how to use them to prevent the impact of harmful spam.

Password policy: The policy should also include provisions concerning requirements regarding passwords for IT devices. In particular, employees should be obliged to set a password which consists of a required number of characters, including lowercase and uppercase letters, numbers and special characters. Furthermore, in order to give greater security, employees should change their passwords

regularly, and important data should be backed up frequently.

Unknown email policy: The policy should prohibit opening any suspicious email and should require that such emails be forwarded to a specialised IT department for assessment. For clarification, all policies should include examples of prohibited or desired actions. Furthermore, even the best IT security policy is useless if employees are not aware of its existence or are not trained on its proper application.

4. Bilateral agreements with employees

Another form of protection against cybersecurity events which is a common and recommended practice is to conclude non-disclosure agreements with employees. Such agreements oblige the employees not to disclose any confidential information covered by the contract. Apart from employees, non-disclosure clauses should be included in all types of contracts with people who may have access to the enterprise's trade secrets. A non-disclosure undertaking can be concluded not just for the period of employment or other access, but also for a period after the termination of employment or other contracts. In such cases, the undertaking may even stipulate contractual penalties or liability for compensation for any breach. However, a provision on liquidated damages may not be valid in every jurisdiction.

5. Training

An important security measure is to expose employees to fake targeted cyberattacks and follow up with training. Nothing works better to focus the minds of employees than to become aware that they were the weakest link. The employer should inform employees that such attacks may be performed without notice and failure to obey the policies may be a reason to impose disciplinary action.

6. Monitoring Software

Employers should consider whether to monitor employees' work. This is becoming an increasingly common method of protection. For example, it is possible to install software such as keyloggers on employees' computers that enables employers to track all activity. Within certain groups of employees, this should be considered a justified form of protection.

On the other hand, most European labour legislation imposes a duty on employers to respect employees' privacy. For this reason, employers should inform employees in advance about using such software or other monitoring measures.

7. Specific Incidents Response Procedure

Every company should develop a plan (cyber incident response plan) that identifies possible cyberattack scenarios and sets out appropriate responses. The plan has to be customised for each company's particular circumstances. Such plan should address the following basic areas: define the response team composed representatives of different departments such as IT, legal, information security, PR, insurance; provide for reporting channels, define the scope and manner of investigation, designate a recovery and follow-up plan and management of public relations and law enforcement.

“ Every company should develop a plan that identifies possible cyberattack scenarios and sets out appropriate responses

8. Consequences

If an employee does not comply with the required procedures, such behaviour may be treated as a breach of its obligations as an employee. Pursuant to most European labour legislation, employees who disobey IT security policy are responsible for the resulting damage to the extent of a material loss sustained by the employer although, in some jurisdictions, during the term of an employment contract, the employee cannot be obliged to pay contractual penalties. Moreover, employers may apply disciplinary penalties with respect to employees who do not observe the rules. In some cases, a breach of duty provided for in the company's IT security policy may lead to termination of the employment contract without notice because it constitutes a violation of basic duties. However, what if the employer has no policies or other measures in place? In most cases, the lack of awareness means that there is limited exposure for and fewer

consequences that may be imposed on the employee. In short, it is the employer's duty to define the scope and means of security.

In summary, the policies should give a roadmap of tasks and responsibilities to manage the risks and to make employees aware that each of them has a role and should strive not to be the weakest link. ■

ANALYSIS

E-RESIDENCY AND DATA EMBASSIES: A COUNTRY WITHOUT BORDERS



PIRET PERNIK

Piret Pernik joined the International Centre for Defence and Security in April 2013. Her research focuses on cybersecurity policy-making and other strategic issues relevant to cybersecurity. Piret's tasks include analysing global developments, including strategies and policies pursued by states and international organisations. She recommends how to shape Estonia's efforts on cyber security and on how to introduce the Estonian experience internationally, as well as coordinates cybersecurity related co-operation with other relevant domestic and international actors.

1. Introduction

Estonia – a small country of 1.3 million people – has become in less than three decades one of the most wired and technologically advanced countries in the world. Estonia ranks high in global indexes measuring technological advancement and cybersecurity maturity. It is:

- fifth country in a global cybersecurity maturity index;¹
- 21st country in the development of information society among 166 countries;²
- seventh country in digital competitiveness and

second in the development of public e-services among the EU member states.³

Estonians are proud of their “e-way of life”. According to official statistics, 95% of people declare their income online (with a prefilled form it may take only five minutes), 95% of prescriptions are issued electronically, 98% of companies' submissions are made over the Internet, and 99% of banking transactions are done electronically.⁴ Estonians have voted over Internet since 2005 (20% of votes were casted online at 2015 parliamentary elections).

1 | Global Cybersecurity Index & Cyberwellness Profiles [online.] <https://www.itu.int/pub/D-STR-SECU-2015> (access: 17.11.2015).

2 | Measuring the Information Society Report 2014 [online.] <http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2014.aspx> (access: 17.11.2015).

3 | European Commission. The Digital Economy and Society Index 2015 [online.] <http://ec.europa.eu/digital-agenda/en/digital-economy-and-society-index-desi> (access: 17.11.2015).

4 | For concise overview about Estonian use of e-services see Estonian Information System Authority. Facts about e-Estonia. [online] <https://www.ria.ee/facts-about-e-estonia> (access 20.11.2015).

Both businesses and citizens consider that e-services help to save money and time. In 2012, 76% of entrepreneurs and 67% of citizens were satisfied with public services.⁵ Currently there are 1.26 million active ID cards, and with electronic identity (e-ID), residents and non-residents can access over 800 public and private e-services or e-applications through the State Portal riik.ee. Among other things, e-ID enables signing legally binding documents and contracts, it gives access to online medical records, and so forth. With the smart ID card individuals can verify who has accessed their records in state databases.

Perhaps not surprisingly, compared to European citizens, Estonian population trust more their personal data to public and private entities (84% of Estonians trust state authorities in regards with personal data and 86% of them trust the private sector). Likewise, they worry less (51% of people) about the state collecting their data than Europeans in average (70% in the rest of the EU), as well as use fewer measures to safeguard their online privacy.⁶

2. Digitalisation and trust

A prerequisite for highly digital society is trust – the users must have confidence that various types of confidential data, as well as transactions with them, are confidential, as well as data integrity and availability is provided at any moment. Keeping trust in “e-way of life” is therefore an utmost goal of the Estonian government and the main goal of its cybersecurity strategy. Estonia learned the importance of keeping cyberspace secure during 2007 cyberattacks, and immediately after the attacks the government adopted national cybersecurity strategy - among the first countries in the world.⁷

But cybersecurity was prioritised prior to the attacks.

In 2006 the work started towards the establishment of NATO Cyber Defence Centre of Excellence (NATO CCD COE) to Tallinn, which received its official status in 2008. NATO CCD COE is a NATO-accredited knowledge hub, think-tank and training facility. More recently, NATO cyber range was set up in Tartu, Estonia. Allies and partners train there annually. NATO's cyberdefence exercise Cyber Coalition that has been held in Estonia since 2013.

“ Keeping trust in “e-way of life” is therefore an utmost goal of the Estonian government and the main goal of its cybersecurity strategy.

3. Public And Private Partnerships

Over the years, state agencies have developed and implemented innovative policies, strategies and legislations concerning IT and cybersecurity. However, a key enabler for technological and cybersecurity innovations has been the presence of strong public-private co-operation tradition - well-established co-operation among commercial, governmental and academic bodies spans over two decades.⁸ The government has supported innovative ideas of entrepreneurs from the private sector, who has funded many public and private partnership (PPP) projects in education, awareness raising, and infrastructure development already since 1990s. In fact, in defending the country against cyberattacks in 2007, effective horizontal co-operation was the key factor.⁹

Estonia was also one of the first countries to launch a voluntary cyberdefence unit (CDU). The idea was approved in 2007, and shortly after an informal co-operation network was initiated. First, it functioned as

5 | Ministry of Economic Affairs and Communications, Green book on organisation of public services, 2013.

6 | Estonian Institute of Human Rights, The right to privacy as a human right and everyday technologies, 2014 [online] <http://www.eihr.ee/en/privacy-as-a-human-right-and-everyday-technologies/> (access 22.11.2015).

7 | In 2007 Estonia experienced cyberattacks for three weeks that targeted prominent government websites along with the websites of banks, universities, and Estonian newspapers.

8 | Kaska, K., Osula, A.-M., Stinissen, J. The Cyber Defence Unit of the Estonian Defence League - Legal, Policy and Organisational Analysis. NATO CCD COE Publications, 2013. p.7, p.37.

9 | Tikk, E., Kaska K., Vihul L., International Cyber Incidents: Legal Considerations. NATO CCD COE Publications, 2010, p. 34.

a “gentlemen’s club”, legal status was received in 2011. The CDU is a national cyberdefence collaboration model integrated into the Estonian Defence League, voluntary paramilitary national defence organisation. It brings together civilians from all spheres of activities (IT, law, economics, and so forth) “to protect Estonia’s high-tech way of life”.¹⁰ One of the goals is to act as a reserve resource pool of well-trained IT specialists who can be deployed to assist in the protection critical infrastructure.¹¹

4. Exporting experience abroad

Estonia is a good example of how cyber means enable less resourceful actors to augment its influence. In foreign policy and economy, the country has set goal to virtually enlarge beyond its physical borders – in 10 years the ambition is to attain 10 million new e-residents. Since 2008 the government has inspired to be a forerunner in international co-operation on cybersecurity, and has shared experiences with others. For example, Estonia and Finland have been developing a joint platform to make digital services mutually accessible. Estonia has used the platform X-road that enables secure data exchange between the state’s information systems, since 2001. Another example is Japan that recently decided to implement smart ID card based on Estonia’s experience.¹²

Furthermore, along with major cyber powers (such as the United States, UK, China, Russia, France and others) Estonia has been shaping states’ future behaviour in cyberspace. Estonia was a member the 2011, 2013 and 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in Context International Security (UN GGE). In fact, it proposed three norms for responsible state behaviour in

cyberspace that were included in the final report.¹³ Similarly, Estonia is a founding member in a network of leading digital governments D5.¹⁴ In NATO, Estonia assumed a leading role in the process of developing NATO’s first cyberdefence policy and has remained active contributor to enhanced approach; within the EU, it has contributed to numerous initiatives to foster cybersecurity.¹⁵

Closer to home, Estonia has prioritized cyber issues in security and defence co-operation frameworks among the five Nordic and three Baltic countries (NB8). Among other things, it initiated annual cybersecurity expert meetings at policy level, and coordinated cyberdefence development assistance projects European Neighbourhood Policy countries.¹⁶

In spite of limited resources, Estonia has become a valued educator in regards with e-governance development and cybersecurity. For example, in 2014 an Estonian non-governmental organisation, e-Governance Academy, assisted 26 countries in adopting e-state solutions; in 2015 Estonian experts provided cyberdefence training to Ukraine state agencies. In Georgia, Estonia supports the development of e-government,¹⁷ and cyberdefence training; In Moldova, Estonia recently organised cyberdefence competition called Cyber Olympics.¹⁸ It is considered that this proactive engagement has increased country’s visibility and influence globally, and granted political capital among partners and allies.¹⁹ This view can be supported by the fact that

10 | Defence League 2014. For comprehensive legal, policy and organisational analysis see Kaska K., Osula A-M., Stinissen J., The Cyber Defence Unit of the Estonian Defence League [online] https://ccdcoe.org/sites/default/files/multimedia/pdf/CDU_Analysis.pdf (access 20.11.2015).

11 | Pernik, P., Tuohy, E. Interagency Cooperation on Cyber Security: The Estonian Model, [in:] Effective Inter-agency Interactions and Governance in Comprehensive Approaches to Operations, STO-MP-HFM-236, April 2014. NATO Science and Technology Organisation.

12 | Estonian Government. Japan to implement ID card following Estonia’s example. [online] <https://valitsus.ee/en/news/japan-implement-id-card-following-estonias-example> (access 20.11.2015).

13 | In 2015 Estonia proposed three norms that were adopted in a consensus report signed by experts from 20 countries: refraining from attacking critical infrastructure, not hindering the work of CERTs of other countries, and providing mutual assistance in case of cyberattacks against critical infrastructure. Pernik P., Maldre P., Rising Challenges: Cybersecurity in the Baltic Sea Region, [in:] Baltic Visions. European Cooperation, Regional Stability, ed. K. Redłowska, Warsaw 2015, p. 48.

14 | The founding members of Digital 5 or D5 are Estonia, United Kingdom, South Korea, Israel and New Zealand.

15 | Areng, L. Lilliputian States in Digital Affairs and Cyber Security. Tallinn Paper No. 4. 2014. NATO CCD COE.

16 | Ministry of Foreign Affairs of Estonia. Estonian leadership in 2014 [online]. <http://bsy.vm.ee/en/nordic-baltic-cooperation/estonian-leadership-2014/> (access: 17.11.2015).

17 | Estonia to train Ukraine cyber experts [online]. <http://news.err.ee/v/International/9b05c491-1eff-49f5-844c-74569a8b80d1> (access: 17.11.2015). Twinning on e-Government launches in Georgia [online]. http://eeas.europa.eu/delegations/georgia/press_corner/all_news/news/2015/20151109_1_en.htm (access: 17.11.2015).

18 | eGA to organize the first Cyber Olympics in Moldova [online] <http://www.ega.ee/news/ega-to-organize-the-first-cyber-olympics-in-moldova/> (access: 17.11.2015).

19 | Areng, L. op cit, p. 10.

number of foreign governments have been looking for Estonia's experience in development of e-government, public e-services, policy and legislation, technical measures, as well as cyberdefence training and exercises.

5. Digitalisation and security

Whereas increasing cybercrime is a global concern, the Baltic region is characterised by politically motivated cyberattacks.²⁰ Russia has advanced cyber capabilities, and a number of Advanced Persistent Threats (APT) that have been attributed to Russian state entities which have been active in the region for many years. Cybersecurity firms and experts have observed increasing sophistication of these APTs.²¹ Elsewhere in Europe and in North-America, state authorities have reported unprecedented leaks personal data, including sensitive data. Cybersecurity firms have pointed out that some APTs have shifted from targeting mainly government and defence related information to seeking personal information.

“ Whereas increasing cybercrime is a global concern, the Baltic region is characterised by politically motivated cyberattacks.

Against the background of the more sophisticated treat vectors and tactics, as well as vulnerabilities related to the growing dependence on IT in every domain of social activity, concentration of large amounts of data may augment these risks. For example Israel plans to transfer biometric data the population into a central database, a move that leading computer scientists have opposed, and the plan is not popular among the general public.²²

20 | Äripäev, Our region is characterised by politically motivated cyberattacks, 21.05.2015 [online] <http://www.ituudised.ee/uudised/2015/08/21/taimar-peterkop-meie-regioonile-on-iseloomulikud-politiliselt-motiveeritud-kuberrunnakud> (access 23.22.2015).

21 | Maldre, P., The Many Variants of Russian Cyber Espionage [online] <http://www.icds.ee/blog/article/the-many-variants-of-russian-cyber-espionage-1/> (access 23.11.2015).

22 | Israeli cyber experts call on government to cancel planned biometric ID system [online] <http://www.biometricupdate.com/tag/israel/>; AlMonitor, Israelis wary of biometric ID cards [online] <http://www.al-monitor.com/pulse/security/2014/09/israel-smart-id-passport-biometric-data-base.html#> (access:23.11.2015).

While acknowledging economic, societal and reputational gains of digital connectivity, it goes without saying that the more digitalised the society is, the more vulnerable it is. In Estonia, dependence on the ICT is steadily growing.²³ Estonian Cybersecurity Strategy 2014-2017, Information Society Development Plan 2020, Estonian Government Cloud Conception 2015, and other strategic documents denote number of ICT risks. First, many critical state databases and services exist only digitally.²⁴ For example, legal acts are only in effect if they have been published online on the State Gazette, and no paper copies of the national legislation are stored. Furthermore, functioning of services depends on other services (e.g. national ID card system), and national databases (e.g. population register²⁵). Another example is land register that contains information of real estate and land ownership. It is also only stored electronically and its evidential value is only in digital form.²⁶ The database contains information on all property relationships dating back to 1994 (in 2010 the change-over to an electronic version was completed).²⁷ The ownership rights are obtained by making a record into the register. If integrity of these databases is lost, the functioning of society may be undermined.

It has been observed that currently state information systems in Estonia are not hosted in datacentres that guarantee high availability and security. State information systems are mostly located in spaces constructed and maintained by the agencies themselves,²⁸ which lack capacity to meet the established standards, thus currently risks are not

23 | Ministry of Economic Affairs and Communication, Cyber Security Strategy 2014-2017 [online] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncss/Estonia_Cyber_security_Strategy.pdf (access: 20.11.2015).

24 | The essential state databases include in addition pension insurance register, state treasury register, e-file system, e-health, and many more.

25 | Population register contains names, ID codes, birth dates, places of residence, and other statistical data such as nationality, native language, education, and profession of each person who lives in Estonia. The register is connected to other systems via the X-road, and a variety of other state services depend on the data in population register. When people apply for allowances, data is retrieved from the population register. Population register [online]. <https://e-estonia.com/component/population-register/>.

26 | Kotka,T., Liiv, I., Concept of Estonian Government Cloud and Data Embassies. Springer International Publishing Switzerland 2015, p. 152.

27 | [European e-justice. What information does the Estonian land register give? [online] https://e-justice.europa.eu/content_land_registers_in_member_states-109-ee-maximizeMS-en.do?member=1 (access: 20.11.2015).

28 | Kotka,T., Liiv, I., op cit., p. 151.

sufficiently mitigated.²⁹ Estimably 60% of server rooms do not meet established information security requirements,³⁰ and many state agencies do not perform regular security audits.³¹

In order to mitigate risks related to state information systems and databases, there is a need to consolidate them into more secure and efficient datacentres that comply with the standards. Furthermore, the establishment of government cloud would help reduce the existing significant duplication between the state agencies in providing ICT services in their administrative areas, as well as save maintenance costs.³² The CyberSecurity Strategy 2014-2017 stipulates that by 2017 all essential state registers must be constantly updated and mapped, as well as have mirror and backup alternatives.³³

Another vulnerability identified by strategic documents is reputational loss that may result from defacement or denial of service attacks against websites with symbolic status like website of Estonian Parliament, President, Government, Ministry Defence, etc. These “digital monuments” need also extra protection because some do not have the requisite level of protection.³⁴

5.1 E-Residency

A winner of the best Estonian e-service in 2015, e-Residency programme has received notable international media coverage and has even been called a “government start-up”.³⁵ The government plans to promote the programme abroad (for example 160 000 euros will be spent on such campaign in the

United States).³⁶

The programme offers to citizens of other countries access to public and private services in Estonia.³⁷ E-Residents can sign with smart ID card, digitally documents (necessary for conducting business in Estonia), report taxes to an Estonian authority, execute bank transactions, etc.³⁸ There are currently 6000 e-Residents who run over 500 companies, and during the first year of the programme, 220 new companies have been established.³⁹ It has been estimated that 30 000 new e-Residents will bring 60 000 euros revenues to the economy. The ambition is to reach up to 10 million e-Residents by 2025. However, success of the programme depends on

“ For e-Residents the availability of services must be provided also in case of losing the outside Internet connection during crisis

the accessibility of services and security of personal data and business transactions of e-Residents at any time, also in crisis. If an individual owns a company in Estonia, he or she must be able to prove the ownership in order to conduct transactions with it. As discussed above, the functioning of services depends on state databases (e.g. commercial register, land register). Even though essential data of the state is backed up in Estonian embassies abroad, currently backups are not frequent enough, thus necessary information may not be available. For e-Residents the availability of services must be provided also in case of losing the outside Internet connection during crisis (e.g. due to cyberattacks, local natural disasters, armed conflict). For example, Estonia temporarily

29 | Agenda of the Cabinet meeting, 2015 [online] <https://valitsus.ee/et/uudised/valitsuskabineti-noupidamise-paevakord-13> (access 21.11.2015).

30 | Ministry of Economic Affairs and Communication, Estonian Government Cloud Concept, 2015, p. 5.

31 | Estonian Data Protection Inspectorate, About the Application of Public Information Act and Personal Data Protection Act in 2014 [online] http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf (access: 20.11.2015).

32 | Kotka,T., Liiv, I., op cit., p. 152.

33 | Ministry of Economic Affairs and Communication, Cyber Security Strategy 2014-2017. [online] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncss/Estonia_Cyber_security_Strategy.pdf (access: 20.11.2015).

34 | Ibidem.

35 | Estonia's CIO: E-Residency coming to Singapore and running a government startup [online]. <http://e27.co/estonia-s-cio-e-residency-coming-singapore-running-government-start-up-20150921/> (access: 20.11.2015).

36 | Estonia is looking for a partner for campaign to introduce e-Residency in the United States [online] <https://www.ria.ee/estli-otsib-partnerit-eresidentsuse-tutvustamiseks-usas/> (access 22.11.2015).

37 | For more information see Estonian e-Residency [online] <https://e-estonia.com/e-residents/about/> (access: 20.11.2015).

38 | Some domestic regulations still need to be changed for the full functioning of the programme. Estonian address is needed to start a company. To open a bank account, an individual must be physically present at the bank.

39 | Real time statistics on e-Residency is available online <https://app.cyfe.com/dashboards/195223/5587fe4e52036102283711615553>.

blocked incoming traffic in responding to cyberattacks in 2007 that rendered Estonian websites (news portals, state agencies websites, online banking) unavailable from abroad.⁴⁰

5.2 Data Embassies

Data Embassy is a catchword used to designate essentially what is government cloud. The Estonian Government Cloud policy 2015 (approved by the cabinet of government ministers in principle), proposes three-step approach in order to solve the above deficiencies:

- to establish government cloud in Estonian territory that meets the established security standards;
- to migrate and host public or non-sensitive state data (e.g. "digital monuments") into a privately owned public cloud (e.g. Microsoft Azure cloud computing platform, which since 2009 hosts Estonian official tourist information website visitEstonia.com of the Enterprise Estonia);
- in addition to backing up essential data in Estonian embassies abroad sensitive data will be stored in dedicated government datacenters in friendly foreign countries.

It is considered that these steps will improve data confidentiality, availability and integrity, but also provide the availability of data and services in local crisis⁴¹ since the key benefit of cloud computing is greater resilience in the face of regional power cuts or local natural disasters.⁴² However, also in case of an armed attack or military invasion the government can continue functioning in exile, while state databases hosted abroad can also remain functional - "virtual embassies will ensure the functioning of the state, regardless of Estonia's territorial integrity."⁴³ It is hold that this approach will ensure digital continuity of the state, it will mitigate risks related to ICT, augment information security

capacity of state agencies, support the development of innovative and high-grade e-services, enable the establishment of a "borderless state" and increase cost-effectiveness.⁴⁴ Also, the European Union Agency for Network and Information Security (ENISA) holds that this "three-step" approach is "a strong foundation for the government cloud".⁴⁵

The cloud is planned to gain full operability by 2018. In addition to storing essential data in Estonian embassies and public clouds abroad, the first phase of the project includes the procurement of space in a government datacentre in a friendly state outside Europe.⁴⁶ This fall, a pilot project with Microsoft was completed. Some non-sensitive, but symbolically valuable state websites were migrated to Azure cloud and the project team concluded that government e-services can be run in a public cloud. The analysis also suggested that in Estonia some national regulations and policies must be revised, and advised further investigation on how international law should be interpreted in specific cases.⁴⁷

“ Key issues to analyse for migration of data onto clouds are security and privacy.

5.3 Cyber security considerations

Key issues to analyse for migration of data onto clouds are security and privacy. The main security challenges are related to data protection and compliance, interoperability, access management, auditing, risk management, etc.⁴⁸ ENISA recommends state authorities to conduct comprehensive risk analysis and estimate whether migration of data outside national borders and territory of the EU may

40 | Tikk, E., Kaska K., Vihul L., International Cyber Incidents. Legal Considerations Estonia 2007 [online].

41 | Ministry of Economic Affairs and Communication, op cit., p. 6.

42 | ENISA. Critical Cloud Computing. CIIP Perspective on Cloud Computing. 2013.

43 | Kotka,T., Liiv, I., op cit., p. 152.

44 | Agenda of the Cabinet meeting, op cit.

45 | ENISA, Security Framework for Governmental Clouds. All steps from design to deployment. February 2015, p. 20.

46 | Kotka,T., Liiv, I., op cit, p. 161.

47 | Ministry of Economic Affairs and Communication, Microsoft, op cit., p. 6.

48 | ENISA, Security Framework for Governmental Clouds. All steps from design to deployment, op cit., p. 8.

impair privacy and security of its citizens.⁴⁹ In order to comprehensively assess the challenges, ENISA recommends national governments to prepare a national strategy for clouds, to include a defined risk management program, as well as to adopt baseline security measures.

As of today, only two member states (the UK and Spain) have defined and implemented a national wide cloud strategy.⁵⁰ Governments propose different measures to secure data in clouds: specific security certification frameworks, risk management baselines (for example, Greece defines a set of baseline requirements), risk assessment frameworks, and use model contracts.⁵¹ There is no standard solution or specific measures that would depend on national circumstances. The Estonian cloud policy outlines main technical, legislative and policy steps to be taken in the near future. It is planned to apply the principles and guidelines on the secure use of clouds for the state agencies and vital services by the end of year.⁵² Likewise, concerning migrating data outside the territorial borders of Estonia, preliminary technical standards and procedures have been formulated and the development of legal aspects is also in process.⁵³

5.4 Privacy concerns

Data should be migrated into different types of clouds (public, private, hybrid) according to categorisation. For example national health or population register that include sensitive personal data cannot be hold in public clouds. In Estonia it has been alleged that in case of serious crisis even sensitive data may need to be migrated to public clouds regardless of the risk to confidentiality. The government may decide so if data integrity is in danger. Indeed, the EU

49 | ENISA, Security and Resilience in Governmental Clouds 2011 [online] <https://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds> (access 22.11.2015).

50 | Ibidem, p. 31.

51 | Microsoft, Transforming Government: A cloud policy framework for innovation, security, and resilience. White paper, October 2015 [online] <https://blogs.microsoft.com/cybertrust/2015/10/22/transforming-government-presenting-a-cloud-policy-framework-for-innovation-security-and-resilience/> (access 22.11.2015).

52 | Mibidiem, Work plan of the Estonian Information System Authority 2015 [online] https://www.ria.ee/public/RIA/Dokumendid/RIA_tooplaan_2015.pdf (access 21.11.2015).

53 | Ministry of Economic Affairs and Communication, Microsoft, op cit., p. 16. Kotka,T., Liiv, I., op cit, p. 161.

directive on the protection of personal data⁵⁴ allows a number of exceptions in transfers of personal data to a third country also when protection of data cannot be guaranteed (e.g. when transfer agreements are in place or in case of public good). In any case the legality of storing sensitive personal data in public clouds needs to be further analysed. Risk analysis should analyse questions such as: who can accesses data, who is liable and controls it, the procedures for supervision, auditing, and so forth, especially if sensitive data is located in another country's jurisdiction. For example, Microsoft's white paper on government cloud policy outlines some general principles related to the protection of personal data stored in clouds:

- data must be protected from unauthorised access;
- control over data must be addressed;
- data needs to remain confidential at any time whether in rest, in process or in transit;
- data should be categorized by sensitivity, etc.⁵⁵

“ Data should be migrated into different types of clouds (public, private, hybrid) according to categorisation.

6. Conclusion

Estonia has got a highly digitalised society. Thanks to its small size and the lack of legacy technology, it is an ideal testing ground for novel ideas. Other countries can learn from Estonian experiences. Estonia can be regarded as largely successful in extending its visibility and influence in terms of digitalisation and cybersecurity in the Baltic and Nordic regions, as well as in the EU and NATO. The key factors of the Estonian approach are solid PPP, and the determined and innovative approach of the government towards the adoption of technological and cybersecurity advancements. Two recent examples of innovation,

54 | European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Official Journal L 281 of 23.11.1995]

55 | Microsoft, Transforming Government: A cloud policy framework for innovation, security, and resilience, op. cit, p.13.

e-Residency and Data Embassies programmes, have received notable media coverage. However, their ultimate success depends also on the mitigation of possible risks that are related to cloud computing. Whereas migrating data onto public and private clouds yields beneficial security advantages, prior to doing so, governments should carry out comprehensive risk analysis, as well as legal analysis concerning sensitive personal data. A comprehensive government strategy on clouds with appropriate security measures should be implemented. The strategy should outline technical, organisational, policy and legal measures to secure different categories of data (from public to classified); as well as discuss the exceptions regarding the protection of privacy in emergency situations. ■

ANALYSIS

ADVANCED ATTACKS AND INTEGRATED DEFENCE

EDITED BY: TOMASZ NIEWDANA

Systems Engineer, Fortinet

1. Evolving malware

Malware is a general term that covers a wide range of evil software applications. There are many variants and types of malicious applications. A dozen of harmful and intrusive features are known and already implemented in the latest sophisticated and advanced malware samples.

History of malware is almost as old as old are personal computers. In the beginning of computing the “malware” mainly has been classified as a virus or worms. In the 80’s the viruses has been designed “for fun” – exposing programming skills, or from “personal frustration” reasons – damaging data or operating systems. The “computer virus” was coined to refer to a malicious program written to destroy data or to corrupt computer systems. In the 90’s malware started using evasion techniques and as a result antivirus software became a growing business. The Internet goes to the home users and business ones, so malware started spreading also over the Network. In the early 2000 email based worms used social-engineering strategies to cheat a computer users. Most famous samples as example “I LOVE YOU” generated many infections all over the world in a very short time. In the next years email SPAM was becoming big business, so malware creators made big money on spreading unsolicited email messages. In November 2008 a Conficker worm infected about 15 million computers all over the world. Two years later malware entered in a new age – as a weapon used by government and military intelligence services.

The Stuxnet, Dugu and Flame were professional designed, developed and state-sponsored malicious computer worms. Malware as a tool and weapon becomes a part of advanced and combined attacks. Ghostnet (a botnet deployed in various offices and embassies to monitor the Dalai Lama agenda), Shady RAT (similary Ghostnet but with government and global corporate targets), Operation Aurora

(monitoring of Chinese dissidents’ Gmail accounts in 2009) and Stuxnet (an attempt to disrupt Iran’s uranium enrichment program) in 2010 are just a few high profile examples. In 2013 the world faced a crypto malware (Cryptolocker, CryptoWall and other variants). CryptoLocker encrypts files across local hard drives and mapped network drives with the public key, and logs each file encrypted to a registry key. Next displays a message informing the user that files have been encrypted, and demands a payment through an anonymous pre-paid cash voucher or Bitcoin.

2. Advanced Persistent Attacks

In recent years, these so-called “Advanced Persistent Threats” (APTs) have become so rampant and unrelenting that they are forcing enterprises to question the current security paradigm. Firms are beginning to wonder if it makes more sense to stop focusing on keeping attacks out, and start accepting that sometimes attackers are going to get in, and aim to detect them as early as possible and minimise the damage. An APT is highly targeted at a specific organisation and takes a muted and often slow and prolonged approach to penetrating an organisation, with the aim of gathering intelligence rather than making immediate financial gain. Precise definitions of APT vary but one can get a good idea of its characteristics through its component terms.

Advanced – Cybercriminals behind the threat have a full spectrum of intelligence gathering techniques at their disposal. These may include computer intrusion technologies and techniques, but may also extend to conventional intelligence gathering and profiling methods. Malware can also hunt and phish for specific information from targeted individuals – this information is then used in a second stage attack. Social engineering techniques are often employed at this stage. While individual components of the attack may not be particularly “advanced”, their operators can typically develop more advanced tools. Attackers

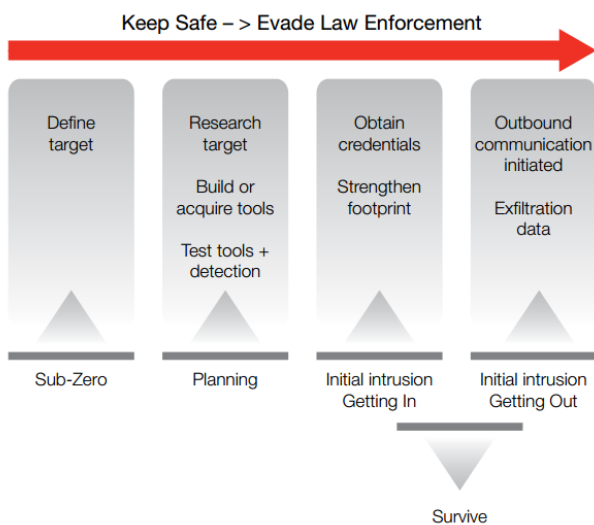
often combine multiple targeting methods to reach and compromise their target and maintain access to it.

Persistent – Cybercriminals give priority to a specific task, rather than opportunistically seek information for financial or other gains. A key requirement for APTs, as opposed to an “everyday” botnet, is to remain invisible for as long as possible. As such, APT perpetrators tend to focus on “low and slow” attacks that let them move quietly from one compromised host to the next, without generating regular or predictable network traffic, to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.

Threat – APTs are a veritable threat because they have both capability and intent. There is a high level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. Cybercriminals target high value assets and they are skilled, motivated, organised and well-funded.

APTs breach enterprise networks through a wide variety of vectors, including Internet-based malware infection, physical malware infection and external exploitation. APT perpetrators do not necessarily need to breach external network perimeters – they can, and often do, leverage insiders and “trusted connection” vectors to access targeted systems.

Fig. 1. The anatomy of advanced threat.



Once the APT attackers get in, certain infrastructure deficiencies in the organisation may facilitate their

obtaining of the desired information: As organisations expand, they combine new and legacy systems, join networks, and integrate with third-party service providers. The complexity created makes it easy for hackers to hide and find unknown or unpatched vulnerabilities. Employee-owned devices and cloud applications add further chaos to the mix. Flat network design is another weakness. While having one broadcast domain cost less, it is more flexible than highly segregated networks, it helps attackers roam the network and possibly reach high-value systems. Business applications typically contain millions of lines of code, making exploitable security holes inevitable. Worse, these software are often not updated with the latest patches to help close holes as they get discovered and fixed. Many security teams are unable to detect sophisticated attack patterns. While conventional tools may identify individual events, they do not associate the events to give a bigger picture. Organisational structure may be another limitation. Security teams are often too soloed to accurately interpret multi-modal attacks.

3. Integrated defense

A layered approach to security can be implemented at any level of a corporate information security strategy. In short, the idea is an obvious one: that any single line of defence may be flawed, and the most certain way to find the flaws is to be compromised by an attack – so series of different defences should each be used to cover the gaps in the other’s protective capabilities. Firewalls, intrusion detection systems, malware scanners, integrity auditing procedures, and local storage encryption tools can each serve to protect your information technology resources in ways the others cannot.

Once malware has breached a network, it will, either automatically or under control of cybercriminals, morph, adapt, and move about undetected for as long as possible, mining data ranging from customer records and intellectual property to device profiles and employee credentials. If security controls cannot detect the malware or its communication during this period, then it is only a matter of time before collected data is staged and exfiltrated, that is, sent back to the

cybercriminal.

A collection of individual security products, however powerful, cannot deliver optimal security if they are acting in isolation. Each piece of the solution needs to work together to deliver optimal protection. Fortinet integrates the intelligence of FortiGuard Labs into FortiGate next-generation firewalls, FortiMail secures email gateways, FortiClient endpoints security, FortiSandbox advanced threat detection, and other security products in its ecosystem to continually optimise and improve each organisation's level security.

Here are the layers that enterprises must have:

Effective protection against multiple attack vectors. This involves a wide-ranging approach to build internal technical controls providing protection at a number levels and vectors, and should include mail, IM, Web exploits, application, malware and botnets.

Robust in-depth asset hardening. This should cover networks, Web applications, data/databases, laptops and servers. The impact of zero-day attacks are best minimised by a combination of keeping patching windows as short as possible, hardening all such assets through robust configuration management based on best practices (e.g. 'least privileges') and judicious deployment of two-factor authentication to critical services.

Application control. This enables enterprises to exercise risk/threat-based application channel, peer-to-peer and botnet control. Employees will be able to safely access social networking platforms like Facebook. Botnet control is particularly important since most modern threats rely on an egress communication channel – blocking communication effectively mitigates many of these threats.

Monitoring. This includes infrastructure-wide monitoring to rapidly respond to any real or potential attacks, as well as up-to-the-minute threat signatures on applications, networks, data and DLP. There are far too many documented cases of threats laying resident on systems and eventually creating millions of dollars in damages, simply because they were allowed to live for months and, in some cases, years.

When mitigating APT attacks, enterprises must be

prepared to deal with highly-skilled hackers with extensive testing facilities and high buying power on the zero-day market. Because an APT hacker can use zero-days and test his binaries against all known vendor engines before sending them to his target, traditional antivirus and intrusion prevention engines likely will not spot the initial attack.

Fig. 2. Cyberthreat Alliance.



This, however, does not mean that firms should not bother installing the relevant security solutions – instead they need to take the additional step of making it hard for hackers to figure out and replicate their environment. It also highlights the fact that human judgement – on things like logs and correlated data – is a prized asset. This judgement, for the time being, is not easily replicated in a testing environment.

The good news about APTs is that an organisation can combat them through its regular risk management process (these protection measures go beyond APTs and also help mitigate traditional threats). APTs simply raise the bar with respect to external risk and impact. How much budget an organisation wishes allocate to tackling APTs will depend, as always, on its appetite for risk. One thing, however, is for sure – top management, CIOs and risk boards around the globe must urgently assess their exposure to APTs and start taking preventive and remediation measures. The so-called holy trinity of security will help enterprises thwart APTs:

1. Educate Users and Keep Security Policies Relevant

Users are generally considered by attackers as the weakest link in the chain, and they are often the target of initial infection. Companies need to educate them on APT infection vectors and social engineering techniques. And, as that will not guarantee that employees will never open an infected document – for instance, Ghostnet got seeded by sending well-crafted and legitimate looking but infected PDF documents to staff of the Dalai Lama’s office – IT managers should make sure that each user has the only access rights that he/she needs and no more. For instance, the office accountant should not have access to the source code repositories.

2. Maintain Up-to-Date Systems

The latest security patches must be applied. IT-wide signature maintenance, typically obtained through a security services provider, includes making the zero-day window as short as possible to reduce vulnerability and operational risk.

3. Adopt “Intelligently Redundant” Security Strategy

Enterprises need to take a multi-disciplinary and consolidated approach to secure all IT assets. Antivirus and intrusion prevention capabilities are essential but firms should consider data loss prevention (DLP) technologies too, and look at the big picture when it comes to the threat landscape. True mitigation results in a blend of policies and protection against the full threat spectrum. Antispam, Web filtering and application control all do their part to block APTs during different stages of attack. The rule of a thumb is that no single security layer is foolproof, and integrating them intelligently helps ward off multi-vector threats. ■

**Together with Polish entities
operating in the IT sector, PGZ develops
modern solutions for the Army.**



The Polish Armaments Group is the leader of the Polish industry and one of the largest defence companies in Europe. The Group concentrates more than 30 companies (defence, shipyard, new technologies sectors), which offer their reliable and highly innovative products intended for modern armies. By the participation in the modernisation programmes of the Polish Army, PGZ constitutes a significant component of national security.

OPINION

WANTED: A PRAGMATIC CYBERNETICS AND A NEW ELITE. A NEW FORM OF POLITICS IN CONTEXT OF THE TECHNOLOGICAL CHANGES OF INTERNET OF THINGS



ROB VAN KRANENBURG

Rob van Kranenburg (1964) wrote *The Internet of Things*. A critique of ambient technology and the all-seeing network of RFID, *Network Notebooks 02*, *Institute of Network Cultures*. He is co-founder of *bricolabs* and the founder of *Council*. Together with Christian Nold, he published *Situated Technologies Pamphlets 8: The Internet of People for a Post-Oil World*. He currently works as *Community Manager* at the *EU Project Societal*. He is consultant to *IoT China, Shanghai 2014*. He Chairs *AC8 - Societal Impact and Responsibility in the Context of IoT Applications* of the *IERC*, The European Research Cluster on the Internet of Things. Rob is co-editor of *Enabling Things to Talk Designing IoT solutions with the IoT Architectural Reference Model*, Springer Open Access.

How difficult it is for any of us to deal with ontological changes? We are nearly always caught by surprise. The Russian Revolution, the building of the Berlin Wall and the coming down of it, the painstaking stakeholder coordination that led to the European Union and its fall that one can predict from indicators I will list here. Ontological changes are changes that redefine the 'normal' and the 'real'. We come to realise that what is 'normal' is a negotiated set of practices, as overnight or in the space of weeks and months the ordinariness of everyday life vanishes with each familiar building, bombed to ruins as in today's Syria - or with each thought that we do not in voice but start keeping to ourselves, no longer knowing for whom we can trust. Insecurity, fear and a general hardening in human interaction in public space is the inevitable result. However, the underlying causes of these are lack of understanding and lack of leadership. In this brief text I want to address these topics.

Lack of understanding

Are you reading this at work or at home? It does not really matter. Just ask everyone in your immediate surroundings to go online and book a flight to Vienna. You quickly notice that you all will pay a different price. Now try the same flight in two weeks. The price will change. In fact if you were able to look at the backend of an Ebay transaction you would see that prices fluctuate every second. We are used to living in a world where prices are relatively fixed. At regular intervals we had 'Sales' and how we enjoyed going shopping then.

Are you booking a taxi with Über sometimes? Then you are aware that the profit on your ride is not going

to the local company and local or national taxes that pay for the road.

Are you traveling through AirBnB? How convenient. I have done it myself and greatly enjoyed it. Yet AirBnB does not bring any jobs like hotels do.

What all these companies are doing is gathering data on and through you, attaching metadata to that and building new services on top of that aggregated data that will be built on top of their own services in which you already have invested part of your online identity. That is why they are called Over The Top Players.

The prediction that can be made from these actions is that in three to five years (maybe even sooner) this variable or dynamic pricing will become the default for any transaction and any purchase. Once there were supermarkets with goods carrying fixed prices and discounts. That is 'now'. We think that is 'normal'. Until there are no more prices one day. Through barcodes, QR codes, Radio Frequency Identification¹ and NFC, (Near Field Communication²), you place your smartphone close to the item that you want to buy and receive a price. That price can be based on the weather, your shopping history, the amount friends you have on Facebook, your drinking habits, that you have a job. The important issue here is that our online identities, the markers on which they are built, the algorithms that are at work and the value

1 | Radio-frequency identification (RFID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. https://en.wikipedia.org/wiki/Radio-frequency_identification.

2 | Near field communication (NFC) is the set of protocols that enable electronic devices to establish radio communication with each other by touching the devices together, or bringing them into proximity to a distance of typically 10cm or less. https://en.wikipedia.org/wiki/Near_field_communication.

that is created with them are beyond our personal and beyond public democratic control. It is also the end of the multi-stakeholder model on wages, work, pensions and social systems of unemployment as these actors have no more agency on the key elements in the economic area.

How did this happen? So quickly and so silently?

There is a very simple reason: the Internet and its global interoperability in the TCP/IP protocol. Never before in the history of mankind was such an operational hegemony achieved. In terms of ontological shifts it is in the category of fire, wheel, book and machine. The book took over 500 years become fully evenly distributed. It was theoretically possible to make everybody literate in Europe by 1500 (and 3 million people), but because royal and theological power stalled it, the first free public book lending in the UK for example was in 1918.

“ Never before in the history of mankind was such an operational hegemony achieved. In terms of ontological shifts it is in the category of fire, wheel, book and machine.

The Internet is based on simple friend-foe logic. Fearing that one swift nuclear attack could take out an entire command centre leaving no more room for response, the US military decided to create an open line between different command centres updating them all in real-time. The gain was certainty that response (revenge) could be delivered. There was price to pay. What in fact was distributed was not certainty, but perpetual uncertainty, as in order feel 'safe', the front door as it were had to be not shut fully, but paradoxically opened wide.

The protocol that was chosen, TCP/IP mimics this deliberate conceptual framework; it was build for resilience, not for optimal security. It basically says

any router: pass on the packet please and does not concern itself with the fact if that really happened or how it happened. It does not care.

Bob Kahn and Vint Cerf, fathers of the Internet together with Peter Kirstein³, wrote, as early as 1988 about Knowbots⁴ 'organisational entities able to reflect upon themselves'. Vint Cerf has worked for Google as Chief Evangelist since 2005. Looking at Google's strategy for the Internet of Things it is clear that his vision has been instrumental.

Internet of Things is in its essence the seamless flow between the:

- BAN (body area network): the ambient hearing aide, the smart T-shirt
- LAN (local area network): the smart meter as home a interface
- WAN (wide area network): Telematics, ITS, Connected Car
- VWAN (very wide area network): the smart city as e-gov services everywhere no longer tied to physical locations

Whoever provides traceability, sustainability and security linking up the gateways (Fog and Cloud) is able to offer the best possible feedback on physical and mental health, the best possible household decisions based on real time monitoring for resource allocation, the best possible decision making based on real time data and information from open sources and the best possible alignments of local energy providers with the global potential of wider communities.

Google is rolling out Glass and Lens, the Google Power meter and NEST, the Car and automotive, open data initiatives, and cultural hegemony through google.org.

As an end-user you will not pay one set of service providers for your health, another for your home,

3 | <http://www.theinternetofthings.eu/rob-van-kranenburg-marconi-society-celebrated-peter-kirstein-carefully-crafted-balance-hard-and-soft>.

4 | <http://www.theinternetofthings.eu/rob-van-kranenburg-marconi-society-celebrated-peter-kirstein-carefully-crafted-balance-hard-and-soft>.

another for your mobility and another for all your services that you receive for being a public citizen. No, you will pay a lump sum, you will lease the full scenario based on data-mining your full spectrum data to one party; read Google and partners.

Effectively the Internet and the Internet of Things combined result in a full re-evaluation of power. As data is the new gold in the 21st century, the full source of soft and hard (in terms of investments in energy, drones, robotics, quantum-computing and nano-bio) power shifts to Silicon Valley.

For the EU and the Member States already in a crisis and budget cut mode for the past decade this means that, as already of the services of the EU citizens are in the hands of these Over The Top Players, as it has no social networks, hardware integration, nor vision on Internet of Things, it has no more legitimacy to ask its citizens to pay taxes as it will no longer be able create added value, nor have the funds to update the infrastructures.

Lack of leadership

Rarely have elites been timely and decisive. The German Kreisau Circle has laid some theoretical foundations that it can be argued for the current paradigm of local and peer to peer, as it focused on an extremely decentralised Germany in an equally decentralised but still united Europe, building on a horizontal scaling of local communities that would share infrastructure and resources. This mix of Christian inspired philosophers, Army officers weary with SS brutality (but a large part of them did not condone the Blitzkrieg), and German nobility adhering to a certain style and strong values of service, was not very well organised but it was the logical context for the von Stauffenberg attentat and subsequent brilliant conception (but lousy execution) of hiding a revolution within an existing official plan for countering a revolution.

The Russian Beseda Circle loosely organised itself some fifteen years before the 1905 Winter palace massacre that turned the popular tide against Czar

Nicholas II. It consisted of a wide range of extremely conservative nobles, socialist and liberal gentry as well as the oldest families in the Russian Empire united in their common belief that without real reform and real changes in the decision making structures of the country it would lead inevitably to bloodshed and breakdown. These were no Kropotkin's or Tolstoy's, they had no anarcho-communist vision at heart and were largely motivated by self interest. Yet they made the same analysis as the anarchists, Lenin and the communist revolutionaries.

There was no more common sense or balance in the systemic architecture that could be supported by convincing structural belief system from which an everyday ethos for practical living could be derived and sensible business models could be deducted. The story had dried up, the protagonists were no longer believable to the audience nor the critics, the actors nor the author and even the props started complain.

The Beseda Circle was not able to organise a space where all parties could feel comfortable for a while. Although not persecuted by Nicolas (as the members were too close to him) the Circle was banned and would never be productive. For the anarchists and communists it was nearly impossible at that time, without data, without an Internet, without social networks, cheap hardware, software, data space storage and analytics, to see that there was a deep common interest between the Black Hand and the Beseda Circle. And as a new ontological space was born, it was filled with blood and violence and petty minds.

A few years ago we were looking for a relatively small amount of money to invest in one of the first EU IoT platforms. We went to the top of the Commission and through them, to old EU VC money. EU VC said: there is no business case. The company was since bought by an American company and it is doing very well. Time and time again we experience that there is no EU mentality, responsibility or 'style'. There is no attempt to keep EU startups European. The idea that Europeanness might be a set of values worth fighting for does not have a strong voice in an elite.

The notion of what constitutes an elite changes. It has acquired a negative connotation of exclusion. However, elites historically are diverse, in flux and organized around a particular intelligence or sensibility able to read the sign of the times. It is the task elites to be a bridge between sclerotic systems and innovation. Rarely have elites aspired to rule themselves and when they did it was always fatal as the #1 position does not suit them. In the days of strategy and tactics, time operating on the side of the young and “new”, space on the side of old and invested powers of place and resources, courses action seem to be clear. Our current EU leadership is mistaken in thinking it is still operating in the conceptual realm of strategy (space) and tactics (time), whereas what has really happened already is the shift to realtime-in-the-network.

“ Our current EU leadership is mistaken in thinking it is still operating in the conceptual realm of strategy (space) and tactics (time), whereas what has really happened already is the shift to realtime-in-the-network.

Two years ago I was invited to the GFF Forum in Rome by the US State Department and the Italian Intelligence Community to talk about Internet Things. The outcomes of the breakout sessions of the somewhat 150 intelligence and security professionals describing the 5 major current threats were one military, two DIY biology and twice the total breakdown of society because of the inability of the state to deal with the digital was the key scenario.

Throughout history it is clear that when there is no more alignment between the intelligence services and the political models that they are supposed to serve, uphold and secure, the end of that system is nigh, in fact it is already dead. That knowledge is just not evenly distributed. And the last ones to know are the

first to go when the time comes. When that happens the newspapers shout: ‘The Wall has come down! What happened? How is this possible?’

So where is the agency? What is to be done?

Currently security has become a container concept. The Cybersecurity paradigm is broken. Cyberattacks cost for example UK businesses £18 billion in lost revenue and £16 billion in increased IT spending per year as a result of these hacks. It is clear that all stakeholders in the industry benefit from the current situation. We have to take the entire system to a new level, with new EU network protocols that do not have the IP dependencies or protocols that are IP friendly. To be clear; we have to break the current Silicon Valley hegemony by breaking the Internet.

In our architectures we are used to dealing with three groups of actors:

- citizens/endusers
- industry/SME
- governance/legal

These all are characterized by certain qualities. In our current (Reference) Models and (Reference) Architectures we build from and with these actors as entities in mind. The data flow of IoT will engender new entities consisting of different qualities taken from the former three groups.

These new entities that should build the governance for these new types of decision making structures. One of these new entities is the Estonian e-card. It has become a service that can be acquired even if you are not an Estonian citizen. Already over 70% services in Estonia, run on the card. It has managed broker massive trust.

If the European Union wants to survive and more actually lead in the 21st century it has to secure its own data. Then It will be able to install, secure and exploit in a public way the above described gateways between the networks. It can thus create its own search engines, taxi services, hotel services,

energy grids etc. In a connected world security becomes a process. As a concept itself it needs to be distributed over the person, the objects affiliated with that person and the immediate surroundings. So any party aiming to do 'security' must have some agency on all these levels. As a 500 million zone it has all the capabilities for scaling horizontally as well as vertically. It could also export this model to Russia, China (already working on a similar 'China OS'), Latin America and Africa.

“ If the European Union wants to survive and more actually lead in the 21st century it has to secure its own data.

I suggest we study the Kreisau Circle deeply as potential guide for a smart Europe. The brilliance the plot on July 20th, 1944 was to hide a revolution in an existing official plan for countering a revolution. What is more logical than to issue EU citizens a smartphone based on the E-Card for a passport the next time you go and renew it? How much more democratic can a system be with every single person on the same level of connectivity and agency?

Using Identity management as a lever, the EU builds a secure, stable and innovative device that acts as a passport as well as a controller to which appliances in the home can be assigned. This device talks specifically to European platforms and a EU Cloud. Citizens gradually manage more of their everyday services in the European service store.

A system without any sense of purpose or dignity can not last.

On the 1st of April 1935 Olga Sjeremetjev was summoned by the NKVD for questioning in the police headquarters in Petrovska street. After two hours of waiting, she was invited into a small damp and smoky room and asked to sit across a man whose face was hid in the contours of an army cap. He asked the usual questions. In between there were long pauses. No one said anything. She could hear the conversations in

the adjacent rooms. People were crying as they were told to pack and leave Moscow in a day, or in two days. After what seemed to her an eternity, he handed her back her passport, told her she was free to leave and maybe she would consider changing her name?

In her diary she writes that she took a tram home, happy to be breathing freely. As she rode through town she kept wondering what the point of this interview had actually been? What purpose does it serve? How does it enable the state to move forward and what does this cost?⁵

Humiliated, persecuted, having watched friends, family and lovers disappear in the horrors of NKVD prisons, she is still able to envisage, in 1935! an ideal "state", much like a 'state of affairs' that has no longer any material grounding, in wondering how much this type of activity actually costs? Not to her, mind you, but to all of us. Olga Sjeremetjev. And no, she will not change her name.

She will not change her name because she has a sense of love and shame; dignity. In the words of the German philosopher Carl Schmitt; we can identify wirkliche Feinde (real enemies) quite easily as they are concrete hurdles, adversaries, situations. There is however the Absolute Feind, die eigene Frage als Gestalt - and this absolute enemy is not infrequently ourselves or some situation quite intimate yet too disturbing to contemplate. To some, it is the loss of personal dignity, to the others it is the loss of soul. Yes, it is quite a paradox that a technical solution should bring the potential for real and honest value given the fact that technical solutions have created the very situation we need to get away from. Still it is the only chance. ■

⁵ | <http://www.theinternetofthings.eu/rob-van-kranenburg-marconi-society-celebrated-peter-kirstein-carefully-crafted-balance-hard-and-soft>.

POLICY REVIEW

COMPETITIVENESS AND INNOVATION IN THE DIGITAL SINGLE MARKET



DR ROLF H. WEBER

Dr Rolf H. Weber is a Professor for Civil, Commercial and European Law at the University of Zurich, Switzerland, and a Visiting Professor at the University of Hong Kong. His main fields of research are: Competition Law, Internet and Information Technology Law, International Business Law, Media Law and International Financial Law. Rolf H. Weber is a director of the European Law Institute and the Center for Information Technology, Society and Law at the University of Zurich, and is engaged in the University of Zurich Research Priority Program about Financial Market Regulation. Besides, he works as an attorney-at-law. His research focus lies on the mentioned topics; the publication list is available at <http://www.rwi.uzh.ch/lehreforschung/alphabetisch/weberr.html>

1. Introduction

The creation of a Digital Single Market has been identified as one of the top ten priorities by the President of the European Commission, Jean-Claude Juncker.¹ On May 6th, 2015, the European Commission has presented a proposition for “Digital Single Market Strategy for Europe.”² In this Communication the Commission has given the reasoning why the EU (European Union) needs Digital Single Market encompassing better online-

access for consumers and businesses across Europe and addressing the cross-border e-commerce rules that consumers and businesses can trust, the affordable high-quality cross-border parcel delivery, the prevention of unjustified geo-blocking, the improvement of access to digital content in a modern copyright framework and the reduction of tax burdens (mainly VAT) when selling products across borders.³ Furthermore, the Commission proposes to create the right conditions and a level playing field for advanced digital networks and innovative services by making the telecoms rules fit for purpose and by implementing a media framework for the 21st century.⁴ Moreover, the regulatory environment for online platforms and

1 | See Juncker J.-C., A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change, Political Guidelines for the next European Commission, Opening Statement in European Parliament, 2014 [online] <http://www.eesc.europa.eu/resources/docs/jean-claude-juncker--political-guidelines.pdf> (access: 03.11.2015), p. 5.

2 | European Commission Communication from 6 May 2015 A Digital Single Market Strategy for Europe (OJ L 192, final) [online] http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf (access: 03.11.2015).

3 | Ibidem, pp. 4-9.

4 | Ibidem, pp. 9-11.

intermediaries must be improved; in addition, trust and security in digital services and in the handling of personal data should be reinforced.⁵

The key direction of the Digital Single Market Strategy of the Commission, however, consists in the strengthening of the digital ecosystem. The likely contribution to the GDP (Gross Domestic Product) of Europe has been calculated at €415 billion.⁶ Thereby, two elements are of major importance, namely (i) the building of a data economy (Big Data, Cloud services, Internet of Things) that are likely increase the competitiveness of the EU industry and (ii) the boosting of wealth maximisation through interoperability and standardisation based on innovative technologies.⁷ These two pillars of the digital ecosystem will be discussed hereinafter.

2. Competitiveness in the data economy

2.1. Market developments

The digitisation of civil society and businesses goes along with the rapid global expansion of Internet access. 3.2 billion people are expected to be online by the end of 2015 of which 2 billion people live in developing countries.⁸ Even if this figure does not cover half of the world population, the further growth will increase the number of connected people and the percentage of these netizens is by far higher within the European Union than on other Continents. Therefore, the (virtual) data economy will continuously gain importance during the next few years.

The access to the Internet and the handling communications and transactions are more and more based on mobile devices. In particular, the younger generation (and the population in developing countries) will be online through mobile

(smart) phones. On September 6th, 2014, the IMF (International Monetary Fund) released its results of the Financial Access Survey, including data on mobile payment indicators. The report showed strong growth of mobile payment in less developed countries, mainly in Africa: depending on the country, quarter or at least one-third of the residents has mobile account.⁹ European businesses can also profit from this tremendous growth of mobile transactions. Furthermore, the generation of data flows has become easy and time-wise not restricted to certain (business) hours. Expectedly, more than 50% of mobile devices will be “smart” by 2018.¹⁰

The most challenging development appears to be the Internet of Things (IoT) being a new source of data exchange in the private domain (e.g. health data) and in the business area (e.g. delivery of goods). According to present estimations, the machine-to-machine IoT is expected to grow in value from \$44 billion by 2011 to \$290 billion in 2017.¹¹ By giving the opportunity to track goods and manage distribution centres, the application of the RFID (Radio-frequency identification) technology in the IoT is substantially improving the efficiency of operations. However, even if the IoT appears to be mainly driven by businesses at this moment, the large generated and collected amount of data is also relevant for private purposes, particularly if the data can be turned into knowledge.¹²

Reality shows that enterprises domiciled in the EU countries do not seem to play a relevant role in the software and hardware sectors (a part from some exceptions, such as SAP and Alcatel Lucent). The main actors come from the United States and China; this fact also makes the European industry dependent from components being produced outside of Europe.¹³

5 | *Ibidem*, pp. 11-13.

6 | *Ibidem*, p. 3; European Parliament Research Service, Mapping the cost of Non-Eu-ropes, 2014-19, 2014 [online] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/563350/IPOL-EAVA_ET%282014%29563350_EN.pdf (access: 03.11.2015).

7 | Communication op cit. (note 2), p. 14.

8 | ITU (International Telecommunications Union), Facts and Figures, 2015 [online] <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf> (access: 03.11.2015).

9 | IMF, Financial Access Survey, Press Release No. 14/425 from 6 September, 2014 [online] <http://www.imf.org/external/np/sec/pr/2014/pr14425.htm> (access: 03.11.2015).

10 | See Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014-2019, 2015 [online] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf (access: 03.11.2015), p. 9; for a general overview see ITU op cit. (note 8).

11 | I Tsai C.-W. et al., Data Mining for the Internet of Things: A Survey, IEEC Communications Surveys & Tutorials 2014, Vol. 16/1, [online] <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6674155> (access: 03.11.2015), p. 77.

12 | *Ibidem*, pp. 77-97.

13 | See also Bendiek A., European Cyber Foreign and Security Policy through Digital Integration, European Cybersecurity Journal 2015, Vol. 1/1, pp. 23-24.7.

However, notwithstanding the global reach of the Internet, new opportunities are not only established for larger firms but also for small and medium sized enterprises (SME); experience in the United States shows that 95% of SME using eBay to sell goods and services are engaged in exports to customers in more than four Continents.¹⁴ This fact is important for the European Union since SME are the main drivers employment and job creation.¹⁵ Furthermore, SME can concentrate their activities to specialised product or service offerings being part of a global value change.¹⁶

2.2. Overcoming market fragmentation through increased competition

Data can be considered as a catalyst for economic growth, innovation and digitisation across all economic sectors.¹⁷ An EU-wide data economy, however, has the problem of overcoming market fragmentation based on different national regimes in order to reach sufficient scale for Cloud computing, Big Data and the Internet of Things. The fragmentation can be caused by technical and/or legislative barriers.

From a theoretical perspective, two main options for regulatory approaches in response to an expansion economic space beyond national borders exist, namely the negative and the positive model approach:¹⁸ The negative integration attempts to remove obstacles to competition and free trade, for example tariffs; thereby a market-creating effect can be realised. The positive integration has the objective to correct market outcomes to the extent necessary and overcome market failure. Both approaches require adequate economic policy coordination and regulatory power in order to realise the Digital Single Market at the EU level. As a specific issue the fact should not be

overlooked that the “traditional” economic transactions in goods are more and more replaced or substituted by trade in services.¹⁹

The available regulatory instruments for the realisation of the Digital Single Market can be grouped into economic regulation, to which sector-specific regulation and competition law belong, and into general legal safeguards, such as data security, data protection or business-related regulations in the information technology sector. Economic regulation embraces two main forms of State intervention being based on two different regulatory regimes, namely competition law and sector-specific regulation:²⁰

(i) Competition law, being usually an ex-post regulation, is characterised by the fact that antitrust authorities intervene if market participants jeopardise free competition by way of restrictive agreements or abusive behaviour in the market. (ii) Sectors-specific regulation is a form of (at least partial) ex-ante regulation, trying to lay the ground for competition; it is only admissible in those markets in which actors fail to provide virtual competition.



The regulatory instruments for the realisation of the Digital Single Market can be grouped into economic regulation and into general legal safeguards

Both kinds of economic regulations have their strengths and weaknesses; it can be said that competition rules are quite general and normally do not provide specific solutions, but are consequently more flexible. In contrast, sector-specific regulation contains precise terms, which offer certainty for regulatory bodies and concerned undertakings; they usually make faster and more effective solutions available.²¹

14 | Ebay, Empowering people and creating opportunity in the digital single market, 2015 [online] http://www.ebaymainstreet.com/sites/default/files/ebay_europe_dsm_report_10-13-15_1.pdf (access: 03.11.2015), p. ii, appendix.

15 | United States International Trade Commission, Small and Medium-Sized Enterprises: Characteristics and Performance, USITC Publications 4189, 2010 [online] <http://www.usitc.gov/publications/332/pub4189.pdf> (access: 03.11.2015), pp. 2-5.

16 | For a general overview see OECD, Top Barriers and Drivers to SME Internationalization, Report, [online] <http://www.oecd.org/cfe/smes/43357832.pdf> (access: 03.11.2015), pp. 7-14.

17 | Communication op cit. (note 2), pp. 14-16.

18 | Bendiek A. op cit. (note 13), p. 23.

19 | See Weber R.H., Digital Trade and E-Commerce: Challenges and Opportunities of the East-Asian Regionalism, Asian Journal of WTO & International Health Law & Policy (AJWH) 2015, Vol. 10, pp. 321-347.

20 | Weber R.H., Legal safeguards for cloud computing, [in:] Privacy and Legal Issues in Cloud Computing, eds. Cheung A.S.Y./Weber R.H., Cheltenham/Northampton 2015, p. 43, pp. 44/45.

21 | Weber R.H., From competition law to sector-specific regulation in internet markets? A critical assessment of a possible structural change, [in:] Competition Law as Regulation, eds. Drexel Josef/Di Porto Fabiana, Cheltenham/Northampton 2015, p. 239, p. 245.

The existence of certain tensions between general competition rules and sector-specific regulation appears to be obvious, notwithstanding the relationship among them and the common objective to realise adequate market structures. Therefore, co-existence applies insofar, as competition rules try to protect competition in general, whereas sector-specific regulation focuses more on promoting entry into markets that are deemed to lack sufficient competition. As a general principle, it may therefore be stated that the existence of – extensive – regulation does not free an undertaking from the obligation to comply with general competition rules.²² In a nutshell, sector-specific regulation and competition rules work together, so the main problem is to find the most effective and well-functioning balance.²³

2.3. Free and secure flow of data

In the Digital Single Market Strategy, the Commission suggests putting more emphasis on a “free flow of data” approach that tackles restrictions on the free movement of data for reasons other than the protection of personal data.²⁴ The Commission also intends to launch a European Cloud initiative including issues such as services certification, contracts, switching of providers and open research facilities.²⁵ The two parallel activities show that the free flow data can not only be perceived as an expression fundamental rights but must also be understood as “network” of legal relations that influence and channel the information distribution.

As practical experience shows, consumers and businesses still do not tend to have enough trust in cross-border Cloud services for storing or processing data in view of the lack of security and compliance with fundamental rights.²⁶ Therefore, the stability and security of the infrastructure must gain importance in the regulatory environment. With this objective,

the European Commission has recommended new rules as means of positive integration related critical infrastructures in the form of the EU Directive on NIS (Network and Information Security).²⁷ Apart from ensuring better IT security, operators of critical infrastructures should become liable for failures and be required to report serious cybersecurity threats even if appropriate safeguards are implemented. As many infrastructural elements are owned by the private sector, national regulators face the challenge of establishing and strengthening the co-operation and the information exchange between public and private sectors, as well as between civilian and military bodies.²⁸ According to the most recent discussions, the risk cannot be excluded that some standardisation and co-operation principles as contained in the NIS draft Directive will be weakened; whether such a development would be beneficial to the European businesses appears to be at least doubtful.

Transparency and access to public data are other elements that can help strengthening the competitiveness in digital markets. Transparency rules are important in the light of the fact that data flows are often restricted in an arbitrary and discretionary manner. If a higher level of transparency is achieved, the likelihood of ameliorating the competitiveness should increase over time. The implementation guidelines for the conduct of States in respect transparency and access to public data is likely improve the digital ecosystem.

3. Innovation through facilitated interoperability and standardisation

3.1. Innovation as social driver

The word “innovation” stems from the Latin verb “innovare” (renew). Usually, innovation is used in connection with new ideas and inventions. The economic theory of innovations has been mainly developed by Joseph Schumpeter; his approach is based on the assumption that economy and society

22 | See Summary Decision, Case T-398/07, EC Commission vs. Kingdom of Spain (OJ 2012 C 138/13).

23 | Weber R.H. op cit. (note 21), p. 246.

24 | Communication op cit. (note 2), p. 15.

25 | Ibidem.

26 | Communication op cit. (note 2), p. 14.

27 | Proposition for a Directive of the European Parliament and the Council concerning measures to provide a high common level of network and information security across the Union from 7 February 2013 (OJ L 48, final).

28 | Weber R.H. op cit. (note 21), p. 246.

are moving towards a change if production factors and production functions are combined in a novel manner.²⁹ In social sciences, innovation is usually linked to creativity.

Further developing the traditional economic theory, innovation should not only concern products and services but also procedures, organisations, business models, designs and even systems.³⁰ At any rate, innovation must encompass a multidimensional approach enshrining novelty and social change. This perception is particularly important in fast moving technological areas; making the complexity of new inventions compatible with the existing value system requires an innovative thinking that exceeds the path dependence considerations.³¹

The new innovations that have been developed in high frequency during the last few years can only extend their benefits to the society if some basic requirements are met. Mainly, innovation will become successful in daily life if the new products and services allow for interchange. This necessity is clear from the variety of innovations, such as: Outsourcing services, Cloud computing, Big Data, e-commerce in general, App economy, social media and websites, streaming services, sharing economy, Internet Things, crowdfunding and -lending. If “combinations” and linkages are not possible, then the single scenarios remain in business silos and are not in position to boost the Digital Single Market. The main requirements in this context are the interoperability and the standardisation.

3.2. Interoperability

The term interoperability can be understood as tool to interconnect networks, but also as a measure to interconnect individuals. The interoperability

(new technologies) means effective interconnection between networks, devices and data repositories.³² Interoperability functions are distinguished on four broad layers of complex systems:³³ (i) The first layer concerns technology (ability to transfer and render the data and other information across systems, applications, or components). (ii) The second layer is the data layer (ability to read the data). (iii) The third layer is the human layer (ability to communicate, for example through a common language). (iv) The fourth layer looks at institutional aspects (ability to work together).

Open participatory standards are usually granting better access to information than a proprietary operating system.³⁴ Therefore, interoperable systems usually make life easier and increase efficiency. The interoperability objective can be reached more leniently if the technology neutrality principle is realised; technology neutrality encompasses (i) the achievement of particular effects (for example related to the behaviour of people or the outcome of activities), (ii) the functional equivalence between different modes of activities (offline and online), (iii) the non-discrimination between technologies with equivalent effects and (iv) the drafting techniques in respect of the developed rules.³⁵

Interoperability is often perceived in a broad sense that includes (i) access to the decision-making process, (ii) transparent and undistorted procedures, (iii) pro-competitive goals, (iv) objective and relevant criteria for technology selection, and (v) no over-standardisation.³⁶ In a more narrow sense, interoperability refers to the possibility of easily linking two different structures.³⁷ Interpreting the Digital Single Market Strategy, it appears to be appropriate to apply a broad approach which allows to make the digital market interoperable for a variety of stakeholders since interoperability is giving rise to benefits for consumers (for example

29 | Schumpeter J.A., *Business Cycles. A Theoretical, Historical, and Statistical Analysis of the Capitalist Process*, New York 1939.

30 | See Meissner J.O., *Einführung in das systemische Innovationsmanagement*, München 2011.

31 | See also Drucker P., *Innovation and Entrepreneurship*, New York 2006.

32 | European Commission, Staff Working Document - A Digital Single Market Strategy for Europe - Analysis and Evidence, Accompanying the document A Digital Single Market Strategy for Europe (OJ L 100, final) [online] http://ec.europa.eu/priorities/digital-single-market/docs/dsm-swd_en.pdf (access: 03.11.2015), p. 64.

33 | SPalfrey J./Gasser U., *Interop: The Promise and Perils of Highly Interconnected Systems*, New York 2012, pp. 5/6.

34 | Weber R.H., *Realizing a New Global Cyberspace Framework*, Zurich 2014, p. 143.

35 | *Ibidem*, pp. 142/43.

36 | Brown I./Marsden C.T., *Regulating Code: Good Governance and Better Regulation in the Information Age*, Cambridge MA, London 2013, pp. 28/29.

37 | Weber R.H. *op cit.* (note 34), p. 144; in general Palfrey/Gasser *op cit.* (note 33).

avoidance of lock-in) and society generally through competition and innovation.

From a theoretical perspective, interoperability issues can be mapped by differentiating between private-sector-led approaches and government-driven measures on the one hand, as well as between unilateral and collaborative approaches on the other.³⁸ In the light of the challenges of the Digital Single Market Strategy, a co-operative approach would be suitable, i.e. the collaboration between the governmental agencies and the private sector on e-commerce matters needs to be enhanced.

3.3. Standardisation

Standardisation can play an essential role in increasing interoperability of new technologies by steering the development of new innovations such as 5G wireless communications or digitisation of manufacturing (Industry 4.0).³⁹ A main difficulty in a fast changing world consists in the keeping pace with the changes in technologies. The previous “bottom-up” process is at risk to undermine the long-term competitiveness. Moreover, international standards should be developed with the aim of underpinning technology developments that are consistent with Internet interoperability. Thereby, standardisation must be implemented in a way that benefits are obtained while minimising any attendant loss of competition.⁴⁰

“ In a world with increasing interoperability of new technologies, standardisation can play an essential role”

Therefore, the Commission has announced to launch an integrated standardisation plan to identify and keep priorities for stabilisation with a focus on the

38 | Weber R.H. op cit. (note 34), p. 144; Palfrey/Gasser op cit. (note 33), p. 14.

39 | See Staff Working Document op cit. (note 32), pp. 64-65; Communication op cit. (note 2), p. 15.

40 | TU, Understanding patents, competition & standardization in an interconnected world, 2014 [online] https://www.itu.int/en/ITU-T/Documents/Manual_Patents_Final_E.pdf (access: 03.11.2015), p. 29.

41 | Communication op cit. (note 2), p. 16.

technologies and domains that are deemed to be critical in the digital single market.⁴¹ Standardisation can also be seen as a vital condition for the stability of the legal framework that is of major importance for the planning horizons of enterprises. In several documents related to the Internet governance issues as well as to a fully functioning Internet, the European Commission has referred to freedom, security and stability as key factors for the long-term maintenance of cyberspace.⁴²

3.4. Additional issues fostering innovation

The Digital Single Market Strategy seems underestimate two issues that will increasingly influence competitiveness and innovation in the digital ecosystem, namely services and payment options.

The Internet is offering increasing opportunities for digital services transactions, for example professional services in the legal, financial or engineering field. In addition, as experience has shown, the distinction between goods and services is blurring as IT software is very obviously evidencing.⁴³ Two major areas of liberalisation are the telecommunications and financial services; abolishing traditional regulations not anymore mirroring the needs of today's society opens the floor for new innovative technological developments.

Even more important is the payment sector that is not tackled in the Digital Single Market Strategy in an adequate way. Payment schemes are becoming the key drivers of the digital ecosystem. The existing legal framework with the E-Money Directive⁴⁴ and the (revised) Payment Services Directive⁴⁵ does not meet the challenges of the next few years. The blockchain technology as used by virtual currencies such as

42 | Bendiek A. op cit. (note 13), p. 28.

43 | See Weber R.H. op cit. (note 19), pp. 325-326.

44 | Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, (OJ L 267).

45 | Proposition for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC from 24 July 2013 (OJ L 547, final).

46 | See Weber R.H./Baumann S., FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien.

bitcoin are most likely gaining a central role in digital transactions. This new technology will also become the foundation of a whole series of FinTech products that play a growing role in the financial markets.⁴⁶ The European Commission would be well advised to pay more attention to the electronic payment schemes being able to substantially boost competitiveness and innovation in digital markets.

4. Outlook

The Digital Single Market Strategy is a very valuable milestone in the development of a stronger digital ecosystem and of an improvement of competitiveness and innovation in the EU markets. Some key points merit special emphasis:

A stable and foreseeable legal framework for cross-border data flows must be established. In 2016, the European Commission will introduce a European Initiative on “Free Flow of Data” that shall provide the free movement of data in the EU; furthermore, a European Cloud Initiative will be launched by the European Commission.⁴⁷

Transparency principles and access to public data need higher attention since national restrictions on free data flows are often implemented in a discretionary manner; in order to drive innovation the access to public data must be a major element of the Free Flow of Data Initiative.⁴⁸

The co-operation between governmental entities and the private sector in the digital ecosystem should be enhanced. Companies as well as individual have the (legitimate) expectation that the digital access public authorities is smooth and “smart.”⁴⁹ According to a recent study on eGovernment, a so-called “digital-by-default” approach in the public sector (meaning that all services are provided digitally) as new strategy

in the EU could cause savings of about €10 billion per year.⁵⁰

In view of the growing importance of services and particular of payments schemes more emphasis must be directed to the implementation of a liberalised regime in these markets since the abolishment of restrictions and the increased technological opportunities have a high potential to boost competitiveness and innovation in the digital ecosystem. In addition, a more coherent regulatory framework and a combined impact of technological developments could have influence on connected markets.⁵¹

In the medium term the development of adequate (online) dispute settlement mechanisms being able to solve controversies in the digital ecosystem appears to be unavoidable. An EU Directive on consumer ADR (Alternative Dispute Resolution)⁵² and a Regulation on consumer ODR (Online Dispute Resolution)⁵³ have been implemented by July 2015. From the beginning of 2016, an EU-wide platform for ODR will be operational;⁵⁴ its influence on the outcome of forthcoming e-commerce disputes may be significant.⁵⁵

The European Parliament and the Council are invited to endorse the Digital Single Market Strategy since the roadmap for completing is quite ambitious; the first actions have already been taken in 2015. The whole process must be done in close co-operation with all stakeholders and require full engagement of the involved parties.⁵⁶ The year 2016 will most likely give good indications when the full implementation of the Digital Single Market can be expected; in the interest of the European businesses it is to be hoped that the digital ecosystem in the EU is realised as soon as possible. ■

47 | Communication op cit. (note 2), p. 15; See European Commission, Outcome of the workshop: Facilitating cross border data flow in Europe – on data location restrictions, 2015 [online] <http://ec.europa.eu/digital-agenda/en/news/workshop-facilitating-cross-border-data-flow-europe-data-location-restrictions-outcome-workshop> (access: 03.11.2015).

48 | Communication op cit. (note 2), p. 15.

49 | See Staff Working Document op cit. (note 32), pp. 64-65.

50 | European Commission, Study on eGovernment and the Reduction of Administrative Burden, 2014 [online] <https://ec.europa.eu/digital-agenda/en/news/final-report-study-egovernment-and-reduction-administrative-burden-smart-20120061> (access: 03.11.2015), pp. 24-25.

51 | Staff Working Document op cit. (note 32), 41.

52 | Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165).

53 | Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165).

54 | http://ec.europa.eu/consumers/solving_consumer_disputes/non-judicial_redress/adr-odr/index_en.htm (access: 03.11.2015).

55 | See Clifford D./Van der Sype Y.S., Fides Fido: Online Dispute Resolution a trusted solution to e-commerce disputes? [in:] Information, Ethics and Security, ed. S. Kierkegaard, 2014, pp. 206-218.

56 | Communication op cit. (note 2), pp. 19-20.

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION AND ORDERING INFORMATION

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 – thank to these features the European Cybersecurity Journal will provide you with an outstanding reading experience, from cover to cover.

In order to subscribe, please send a subscription inquiry via e-mail to editor@cybersecforum.eu with money transfer confirmation attached.



PRICING OF THE ANNUAL SUBSCRIPTION (4 ISSUES)

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

CONTACT INFORMATION

The Kosciuszko Institute

editor@cybersecforum.eu

ul. Lenartowicza 7/4, 31-138 Kraków, Poland

Tel: +48.12.632.97.24

BANKING INFORMATION

Alior Bank

SWIFT: ALBPPLPW

IBAN: PL21 2490 0005 0000 4600 7451 5642

THE ECJ IS ADDRESSED 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
- Military & 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

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



is the publisher of

**EUROPEAN
CYBERSECURITY JOURNAL**