VOLUME 2 (2016) ▪ ISSUE 4

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

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

ISSN: 2450-21113

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

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows: "European Cybersecurity Journal", Volume 2 (2016), Issue 4, page reference

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 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: Marcin Oroń

EDITORIAL

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

It has been exactly one year since the release of the first issue of the European Cybersecurity Journal. In the last 12 months, we have prepared four issues of our quarterly journal with dozens of articles analysing key aspects and the latest problems pertaining to cybersecurity, in a broad sense of the concept. Both feedback from our readers and the enthusiasm of authors confirmed our belief that the need for a platform for sharing knowledge, experience, and in-depth research is strong and pervasive. We, therefore, continue our work with even greater commitment and bring you the next issue of the European Cybersecurity Journal. It is indeed a special edition where we encourage even more strongly to take bold measures aimed at ensuring safe cyberspace.

Cybersecurity is a challenge that must be addressed both holistically and individually. Therefore, it is necessary to take action at global, regional, and national levels as well as at the level of individual actors: companies, organizations, and people. Each of these actors must understand their roles and their specific character, and be ready to take action that will contribute to the building of a cybersecurity system as a whole.

The present issue of the European Cybersecurity Journal and the contents included therein reflect the nature of the problem understood as such and are intended to help achieve the goal of strengthening cybersecurity. The articles contained in this issue of our quarterly journal provide recommendations and guidance on good practices to effectively counter specific threats posed by the network. They also give insight into challenges and behind-the-scenes political actions. We encourage you to read the inspiring interviews carried out with people who tackle the challenges posed by cyberspace from multiple perspectives, which offers a one-of-a-kind opportunity to draw upon their unique experiences and knowledge.

We strongly believe that the knowledge contained in the articles will contribute to deepening skills and enhancing the understanding of issues related to cybersecurity. This is a basic requirement if we are to take advantage of the full potential and opportunities offered by cyberspace in a secure manner.

CONTENTS

INTERVIEW WITH CHRISTOPHER PAINTER

CHRISTOPHER PAINTER
Mr. Painter has been on the vanguard of cyber issues for over twenty-five years. In his current role as the Secretary's first Coordinator for Cyber Issues, Mr. Painter coordinates and leads the United States' diplomatic efforts to advance an open, interoperable, secure and reliable Internet and information infrastructure. He works closely with components across the Department, other agencies, the White House, the private sector and civil society to implement the President's International Strategy for Cyberspace and ensures that U.S. foreign policy positions on cross-cutting cyber issues are fully synchronized.

Mr. Painter is a recognized leader in international cyber issues. He has represented the United States in numerous international fora, including chairing the cutting edge G8 High Tech Crime Subgroup from 2002-2012. He has worked with dozens of foreign governments in bilateral meetings and has been a frequent spokesperson on cyber issues around the globe.

Sir, first of all, thank you for finding time for this interview. I strongly believe that it is crucial to start talking about cybersecurity in an international context, especially that a lot of important processes are currently underway, influencing the international community to a great extent. Based on the decision of the UN General Assembly, a new UN Group of Governmental Experts (GGE) will start its work soon. What kind of an outcome and findings do you expect out of the work of the experts?

To begin with, let me put some context around that. This will be the fifth GGE and I think that the last two in particular have shown a notable progress on a number of issues, the key matter being the applicability of international law in cyberspace as a foundational matter. At the last GGE, a particular importance was paid to the elucidation of what we call "peak time" norms – norms of behaviour of states below the threshold of an armed conflict or, for that part, of international law plug-ins. Those were pretty tremendous achievements, given the core active membership of that GGE. Even more so, in the GGE, there were expert groups in a number of different areas, and the cyber group has become one where it has really been a crucible for producing these very valuable results: the framework that we have championed for some time, international law as the foundation of norms of behaviour, voluntary norms of behaviour, and confidence-building measures. I think that has been a real success.

Even this year we have had it go well beyond the GGE and have the GGE report affirmed in the G20 declaration that came out just a few months ago now. That really shows this has become a real global issue – an important issue. Now, on that foundation, we want to continue with the mandates the GGE has. The focus is predominantly on the international security aspects, so we would like to see a further elucidation on how international law applies to cyberspace, a further discussion of the norms and how we implement those, and also of confidence-building measures, which I should say is beyond the GGE. But I think one of our chief goals over the next

period of time is to do that work in the GGE, and also to get a wider number of countries all over the world, even those outside the GGE, to affirm and to embrace this framework as well as the framework of international law, the framework of norms of behaviour (the ones that we have elucidated), and confidence-building measures. That is a key part of what we want to do. The first meeting of the new GGE will be in August. There are 25 members this year. Some are different than last time, and some are the same, so we are looking forward to that.

I would also like to underline, with respect to the things that have come out of the GGE on this framework in the past, especially confidence-building measures, that we have been making progress in other forms on that. We are doing some efforts to take those forward particularly in the Organization for Security and Cooperation in Europe (OSCE), but also in the ASEAN regional forum. We are both concentrating our efforts on the GGE, but also looking globally to gain a wider acceptance of this framework and do some more practical work on it.

You said that you were looking for a practical implementation of confidence-building measures in different formats and on various regional fora. Do you have any plans to push forward more practical talks, for example, within the framework of the OSCE?

Yes, within the OSCE, we have been doing a lot of work on confidence-building measures recently. About two and a half years ago, we had the first set of 11 confidence-building measures that came out from the OSCE. Just last year, the last additional 5 of confidence-building measures were added to that. The OSCE has been looking at how to implement things like exchanging doctrine among countries, or setting up points of contact, i.e. a number of really practical elements. Confidence-building measures from the OSCE make a lot of sense. Within the OSCE, a lot of its work over the years has been done on these kinds of practical, confidence-building measures, albeit in another context, so it is a perfect venue to discuss these issues.

The Department of State undertakes many actions to implement President's International Strategy for Cyberspace. Could you please describe or elaborate on the greatest achievements so far?

There is a broad sweep of what the international strategy is. It is not just a strategy about cybersecurity. It is a strategy about all the aspects in cyberspace because even though they are distinct, they are also in a relation. So the strategy talks about freedom of expression and human rights in cyberspace, about Internet governance issues and economic issues, about capacity building, cybersecurity, cybercrime, and international security. So there are many achievements in each of those areas and I hesitate to prioritize one of the areas over another because they are so important and they are all different. They also happen to differ between communities. Having that said, I would like to underline that not just creating, but pushing and getting pretty strong acceptance in a short period of time within this international security framework I just talked about – international law, confidence-building measures – is a really big achievement. Diplomacy often moves slowly, but this has been done pretty quickly, hence it is something I would highlight.

I also believe that some organizational things like Internet freedom, the creation and expansion of the Freedom Online Coalition has been very important. In the context of cybercrime, there are a number of new countries who joined the Budapest Convention, and many countries who came up with good cybercrime laws and have increased international collaboration. In cybersecurity, it is worth mentioning due diligence, as we call it. There are many countries now that have created national strategies for cyberspace and

CERTs, and are now collaborating internationally. There are other economic achievements in terms of Internet governance and maintaining the multi-stakeholder system, which has been quite important. So really, across all those pockets, there have been some real achievements I think.

I would like to give an overall comment on some international aspects. Just a few years ago, although I have been doing the job for 24 years now in different capacities, this was seen very much as a boutique or a technical issue, and not so much as a policy issue. But now, firmly in the U.S., but also in more and more countries around the world, this has become a key issue of a national security policy, a human rights policy, an economic policy, and a foreign policy. And we have seen that play out in a couple of different ways. For example, just yesterday we had the Singaporean Prime Minister in town, and the declaration that came out of his visit with President Obama had a very significant statement in respect to cyber issues. Virtually every time our president now meets with a foreign leader, there is a significant statement on cyber issues.

I started this office 5 years ago, and we were the first in the world to have a foreign ministry post in office dedicated to the issues. There are now about 22 around the world. There are dialogues between countries and governments around the world to try to break down the barriers between the different agencies and parts of a country and their private sector from civil society. And that is a huge change in a very short period of time. I think there have been both procedural changes and real substantive achievements. That does not mean, however, that we are done yet. I think that we are still fairly near the beginning of this road and there is a lot more work to be done. Nevertheless, it is heartening to see the level of interest and understanding that we see around the world.

This is exactly why we have decided to create the European Cybersecurity Forum, just to promote the idea that cybersecurity is not purely an IT issue, but a strategic challenge that also needs to be understood from the policy-making perspective. We truly admire your work in this field and your efforts to promote this kind of attitude, and we are doing whatever we can to motivate the CEE region to look at cybersecurity exactly from this perspective.

To illustrate that, for a long time, within governments, there would be a technical minister, or a person in the ministry of communications who would get involved in cybersecurity. But what you see in almost every country now is that a communications minister might have a part, the interior ministry might have a part, the justice system will be involved, the same with the foreign ministry and the defence ministry. So even within governments it is important to see the different aspects. This is a challenge.

Exactly. Sir, you mentioned the promotion of cybersecurity due diligence as one of the areas where your focus is. All nations have responsibility to protect their own networks and information infrastructure, and your department supports these efforts. One of the main pre-conditions of cybersecurity in general is well-working private-public cooperation, so my question is: do you have any advice on how to build solid cooperation between the private and the public sector?

I think there are several things that are important here. Many countries now have and many more are developing national strategies. And with national strategies, we think the best practice of doing those is to consult with the private sector and civil society. It is not just a government issue – it is larger than that. We also have countries that are establishing national CERTs, and those national CERTs obviously plug in with the private sector as well. Even in our own country, when we did our

National Incident Response Plan, for instance, we built it with the private sector from the beginning because they own a lot of important infrastructure. There have been a lot of developments in the U.S., even recently, in terms of engaging the private sector in these issues. We had a summit with the private sector out in Stanford about a year and a half ago. We passed legislation in our Congress to allow better information sharing between the public and the private sector, and took down some barriers. That is important and that is something we promote as we go around the world and say it is crucial to have that engagement with the private sector and civil society.

In addition, we have done a lot of capacity building, particularly in Sub-Saharan Africa, but also in other parts of the world. The OAS in our region has done it in Latin America as well. And we do not just go as the government. We also have private sector representatives who are there talking to countries, so they can understand that it is part of the best practice of how you build it. These are operational issues which are about making sure you are sharing information between the private sector and the government, so you are better able to defend your networks and respond to incidents. There is also the larger policy if the government takes care of designing their policy. The private sector should be someone in our group. It is not monolithic. There are many different parts to the private sector, just like there are many different parts of civil society, or the government. But really having that engagement is important.

My next question is related to the issue that unfortunately has recently become extremely important for Europe, namely a growing risk coming from the use of the Internet for terrorist purposes. In your opinion, how can we fight this problem, this risk, without violating human rights and fundamental freedoms, including privacy? I know the question is very complex and hard to answer, but could you just share your thoughts on that?

We have a very extensive first amendment protection in our system, and all other like-minded countries have freedom of expression as something that the courts value. It is obviously a concern that terrorists are using the same networks as we are to communicate, to plan, to recruit, and to get funded. Now, some of those activities are illegal in our system: if someone is providing material support for terrorism and is funding terrorism – that is something we will go after. But, generally, what we have not seen terrorists do as of yet is to launch attacks against critical infrastructure using cyber means. They have mostly used the Internet to spread their war and communicate plans. What we have been trying to do is to counter the terrorist message: to get to the root cause and counter this very negative message with positive messages, and try to reach that community they are trying to reach. This is here at stake at the Global Engagement Center, and there are also a number of countries doing this together. This countering might not need to be from the government. It might be from other sources, from people within the community of people who are exposed to it. That is something that the State Department has spent a lot of time focusing on, and that is what we will continue to do.

Now I would like to touch upon the Report to Congress on the International Cyberspace Policy Strategy. The document summarises the involvement of the Department of State in the implementation of your international strategy. In this document we can read that countries like Russia or China advance alternative visions for international stability in cyberspace. So could you please explain how this vision differs from the ideas that the U.S. promotes, and how do you deal with this issue? How do you try to resolve the differences?

It is not going to come as a big surprise that there are other countries that have a very different view of cyberspace overall. For example, when Russia uses terms like “information security” and “end-

to-end cyber security", what they are saying is that they want to control information. They often see information itself as a threat, so a lot of their policies will go on that. When you look at Internet governance for instance, if countries want a more state-centric control, they want to do that because they think that it is a better chance of controlling what they think is destabilizing information.

You have command of, from the human rights' and the government's perspective, that absolute sovereignty that we see Russia and China arguing for in a number of different forms. Sovereignty exists in cyberspace. Certainly, there are sovereign aspects of cybercrime – servers are located in countries, etc. But you cannot take sovereignty too far. Sovereignty is not absolute. Things like universally recognized human rights transcend sovereignty. I believe, therefore, we should emphatically counter different approaches. We deal with countries who disagree with us on a number of things. We are having dialogues with China about some of the international security issues, about the theft of intellectual property issues, and cybercrime. It is important to have those dialogues. Nevertheless, I think the big thing for us is that a lot of like-minded countries around the world believe, as we do, that the Internet needs to remain open and uncapped. Adopting a more repressive view of controlling everything is not the way to go.

There are also a lot of countries who are trying to decide what their future is, especially in the developing world. As they get more connectivity, I think it is incumbent on us and other like-minded countries to work with those countries because they understand that there are huge economic and social benefits to the vision that we are promoting over the visions that some more repressive countries are providing. So that is the challenge where we have done a good job so far. And it is not a battle that is going to go away – it will continue to be an issue.

Thank you for pointing this out. I believe that countries like Poland should strongly support all of your efforts aimed at promoting open, secure, and interoperable Internet.

One big signal is that it does not mean we cannot try to find areas of common ground. The GGE report, for instance, reflected the ground that included Russia and China as well as a number of other countries. You have to look for common ground, but you also have to be clear about the differences and highlight why those differences are important and where you want to go.

Confidence-building measures, especially those related to critical infrastructure protection, are one of the examples where countries with different opinions on some of the issues should focus on and seek common ground.

I think the fact we got agreement on some of those norms means that even countries that often disagree with us also see the value in them. But those are not ideologically-based issues. Those are based on a real desire not to have an invert escalation. They are practical and they are meant to be practical.

Thank you so much for your time and answering our questions. It was a huge honour and pleasure talking to you. I hope we will see each other during the next CYBERSEC.

The pleasure is all mine and I very much hope to make it to the next one. ■

Questions by:
Dr Joanna Świątkowska
The Kosciuszko Institute

POLICY REVIEW

DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS: THE ARCANA OF THE EU DECISION-MAKING PROCESS[1]

AGNIESZKA KONKEL
Agnieszka worked for the European Parliament in the years 2012-2015. In the Secretariat of the Committee for the Internal Market and Consumer Protection, she was co-responsible for the negotiations of the NIS Directive and the Digital Single Market in general. Beforehand, she was in charge of the Polish Presidency of the Council when working for the Permanent Representation of Poland to the EU. At the Foundation for Information Society Development, Agnieszka was a part of the highly successful Global Libraries Programme of the Bill and Melinda Gates Foundation. Currently, Agnieszka holds a position of counsellor to the minister at the Ministry of Digital Affairs in Poland.

LĪGA RAITA ROZENTĀLE
is the Counsellor on Cybersecurity Policy at the Latvian Permanent Representation to the EU and the Latvian Delegation to NATO. During the Latvian Presidency of the Council of the EU, she was the Chairwoman of the Council Working Party on Telecommunications and Information Society on the NIS Directive and for the Friends of Presidency on Cyber Issues. Having worked at the Latvian Ministry of Defence on international issues since 2003, Ms Rozentāle has developed a wealth of knowledge in the field of international security, international organisations and cybersecurity. Ms. Rozentāle is a former UN Fellow on Disarmament.

1. Introduction

The EU decision-making process and the negotiations that led to the adoption of the directive concerning measures to ensure a high common level of network and information security across the Union[2] (the NIS Directive) was not always clear outside the walls of the EU institutions. This article attempts to review and explain the mechanisms of interaction between the stakeholders involved to elucidate the challenges involved in reaching a final agreement on the Directive. Although different levels of preparedness, understanding, and interests exist among the Member States, it needs to be acknowledged that the NIS Directive constitutes the first EU-wide instrument of its kind that creates significant European added value. The Directive sets regulatory obligations that aim to create a level playing field, close existing legislative loopholes and consolidate fragmented approaches to cybersecurity created by the Member States with varying levels of capabilities and preparedness. The Directive also sets minimum requirements for the national security of network and information for the Member States to build a better framework for effective cooperation and collaboration[3].

After a formal approval by the European Parliament in July 2016, the implementation clock started ticking: The Member States are to ensure their representation in the newly established the Cooperation Group and the CSIRT Network, meet the deadline for the transposition of the Directive that passes in the first half of 2018, and identify operators of essential services in each of the subsectors outlined in the Annex by the end of 2018. Before we go into detail, however, one should not forget that once the European Commission released its proposal on 7 February 2013, it took eight Presidencies of the Council of the EU and seven informal trilogues[4] before the Directive was finally adopted. The process took over three years to complete, undergoing a series of varying levels of progress as internal and external factors influenced the dynamics of negotiations.

1 | The views and opinions of the authors (acting in their private capacity) expressed herein do not necessarily state or reflect those of the governments represented.

2 | European Commission, *Directive concerning measures to ensure a high common level of network and information security across the Union*, 2013 [online] https://ec.europa.eu/digital-single-market/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and.

3 | See the NIS Explanatory statement of the European Commission.

4 | Informal tripartite meetings attended by representatives of the European Parliament, the Council and the Commission.

2. NATO

The adoption of the NIS Directive comes at a time when other international organisations are also actively addressing different aspects of cybersecurity. When the European Commission first published the proposal for the NIS Directive in 2013, NATO was also looking at the cyber defence needs of the Alliance.

> “Both the EU and NATO share the view that cybersecurity is not only a matter of national security, or an economic or social issue, but also a problem that needs to be addressed across all areas of policy making.

At the Wales summit in 2014, NATO endorsed an Enhanced Cyber Defence Policy noting the fact that “cyberattacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability”[5]. The statement makes it clear that both the EU and NATO share the view that cybersecurity is not only a matter of national security, or an economic or social issue, but also a problem that needs to be addressed across all areas of policy making. No individual document, policy, or a piece of legislation can begin to work towards a solution to an exceptionally horizontal issue.

In the area of cyberdefence, progressive steps towards strengthening the cybersecurity of NATO networks and those of the Allies continued. On 8 July 2016, two days after the NIS Directive was adopted by the European Parliament, NATO allies’ heads of state and government met at the NATO Summit in Warsaw to take new strides towards enhancing NATO’s cyberdefence capabilities. Several significant decisions were taken at the Summit that would greatly affect the general state of cybersecurity in the EU. While it is generally believed that NATO focuses on strictly military issues and the EU, with a few exceptions, on common civil policies, several parallels can be drawn between the decisions taken at the Warsaw Summit and the progress the NIS Directive hopes to achieve. Additionally, many EU Member States and NATO allies do not draw strict divisions between the way cybersecurity is addressed nationally and the manner in which military and intelligence institutions overlap with civilian organisations in order to address cybersecurity threats. The economy and society will also benefit from implementing the commitments made in Warsaw.

In Warsaw, NATO allies reaffirmed and strengthened their commitment to their national cyberdefences with the Cyber Defence Pledge and recognised cyberspace as a military domain. While the recognition of cyberspace as a military domain and the strengthening of national cyberdefence capabilities may not initially appear to have a direct impact on the progress planned to be achieved with the NIS Directive, there are areas where overlaps will occur. For one, the cooperation with industry necessary for both cybersecurity and cyberdefence increases the trust and cooperation that are essential to have a coordinated and comprehensive approach to cybersecurity across the EU or, in the case of NATO, the Euro-Atlantic area. If required, the NIS Directive foresees the involvement of private stakeholders to provide input to the Cooperation Group comprised of representatives of the EU Member States. The communique issued at the NATO Warsaw Summit also reiterated the importance of public-private cooperation through the NATO Industry Cyber Partnership (NICP). The NICP has been established specifically to increase cooperation with the most innovative industries within the borders of NATO.

5 | NATO, *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*; Press Release 120, 2014 [online] http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease

Consequently, the most innovative industries in cybersecurity are most often small and medium enterprises (SMEs). By supporting SMEs, NATO also enhances the cybersecurity industry of the EU, and contributes to the economic well-being of the Digital Single Market of the EU.

Lastly, the enhancement of "the cyber defences of our national networks and infrastructures" and the improvement of NATO's "resilience and ability to respond quickly and effectively to a cyberattack"[6] correlate directly with Annex I of the NIS Directive whereby the need to ensure a high common level of security of network and information by improving and reinforcing the computer security incident response capability, albeit in different sectors, is addressed.

3. Fragmentation of the Single Market: The Emperor's Not-So-New Clothes

Varying levels of capabilities and preparedness across the EU is not a new phenomenon. Already in 1980s, when the Albert-Ball and Cecchini Reports of 1983 and 1988 coined the concept of "the cost of non-Europe" in an attempt to frame and quantify the significant potential economic benefits of the completion of a single market in Europe, the idea emerged in the political discourse. The authors postulated that in a specific sector, in the absence of common action at the European level, the efficiency loss to the overall economy and/or collective public good that might otherwise exist, would not be achieved[7]. In accordance with the principle of subsidiarity, it is the responsibility of the EU to legislate in areas which have a sufficient European or cross-border impact. Legislative gaps might appear in a situation when the thresholds of cross-border effects are not clearly defined or measured, which can lead to ambiguity as to how law is implemented in the Member States and to what extent the legislative actions meet the objectives for which they have been introduced. Thus, the source of such legislative gaps might be stemming from historical legacy or from new technological developments. As a result, there are a number of issues which so far have not been regulated at the EU level or have been intentionally postponed[8].

In the case of cybersecurity, according to a study of BSA Software Alliance[9], considerable discrepancies exist between Member States' cybersecurity policies, legal frameworks and operational capabilities, which create cybersecurity gaps in the European Union. It appears that only 19 (20 according to a latter study[10] of ENISA) out of 28 Member States of the EU have cybersecurity strategies in place, while eight have not declared such a framework at all. The quality of existing strategies differs as well. Many remain vague and high-level, lacking a clear implementation plan, as the study notes. Critical information infrastructure protection (CIIP) is a key priority in most of the strategies (15 out of 20 Member States have an objective to protect their critical national infrastructure); however, the approaches taken differ and so does the effectiveness of the methods applied.

There is a common agreement regarding the fragmentation in the EU cybersecurity landscape and the need to bridge existing legislative gaps. However, comparable data, which would enable the measurement of progress

6 | NATO, *Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*; Press Release (2016) 100, 2016 [online] http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

7 | European Parliament, *The Cost of non-Europe in the Single Market. Cecchini revisited*, 2014 [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510981/EPRS_STU(2014)510981_REV1_EN.pdf.

8 | European Parliament, *The Cost of non-Europe in the Single Market*. Part III, Digital Single Market, 2014 [online] http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2014)536356.

9 | BSA Software Alliance, *EU Cybersecurity Dashboard A Path to a Secure European Cyberspace*, 2015 [online] http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

10 | ENISA, *Critical Information Infrastructures Protection approaches in EU*, 2015 [online] https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf.

in the Member States and in different sectors against the set objectives and targets, is scarce. Such empirical evidence would allow progress to be measured against a baseline, which the NIS Directive attempts to introduce. Furthermore, some consider developing and conducting regular maturity assessments of Member States' readiness a worthwhile exercise. Such information could serve as an indication for future actions and ensure fact-based comparability between the Member States, as indicated in a recommendation for the European Commission stemming from a recent study[11].

> "Some consider developing and conducting regular maturity assessments of Member States' readiness a worthwhile exercise.

In line with the Member States[12], the OECD advised that the digital security risk should be treated as an economic rather than a technical issue and, at the same time, be a part of an organisation's overall risk management and decision-making process. In addition, the OECD postulated that policy and technology innovation should be a key to reducing security risks. An interesting insight into the varied levels of innovation across the EU has been given by the European Innovation Scoreboard[13] published in July 2016.

Figure 1. European Innovation Scoreboard country ranking. Source: European Commission 2016.

The main findings of the scoreboard indicate that over the next two years the EU innovation performance in expected to improve and the majority of companies plan to maintain or increase the level of investment in innovation over the next years. It emerges that Sweden is the leader of innovation in the EU, followed by Denmark, Finland, Germany, and the Netherlands. The fastest growing innovators are Latvia, Malta, Lithuania, the Netherlands, and the UK.

Despite the scarcity of comparable data, a though-provoking insight into the condition of ICT security in the private sector across the EU is given by a Eurobarometer[14] survey conducted in 2015 and published in 2016. The survey indicates that in 2015, only 32% of enterprises in the EU-28 had a formally defined ICT security policy, with the shares of over 45% being registered in Sweden and Portugal (51% and 49% respectively). The presence of the ICT security policy in the enterprises means that the sector is aware of the importance of the systems and related risks. It comes as no surprise that these are large

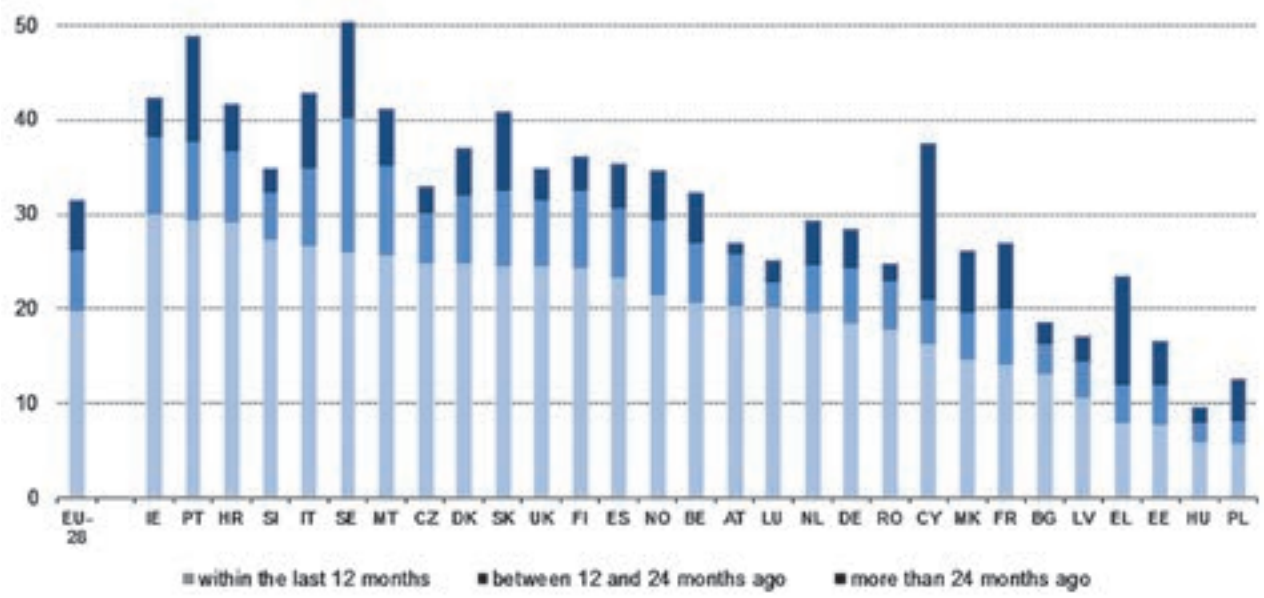
11 | ENISA, *Stocktaking, Analysis and Recommendations on the protection of* CIIs, 2016 [online] https://www.enisa.europa.eu/publications/stock-taking-analysis-and-recommendations-on-the-protection-of-ciis.
12 | OECD, *Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document, 2015* [online] http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf.
13 | European Commission, *European Innovation Scoreboard, 2016* [online] http://ec.europa.eu/growth/industry/innovation/facts-figures/scoreboards_pl.

14 | Eurostat, *ICT security in enterprises*, 2016 [online] http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises.

enterprises which had a formally defined policy for ICT security, their ratio being three times higher than in case of small companies. Generally speaking, the highest proportion of companies which have defined or reviewed their ICT policy in the last 12 months can be found in ICT sector.

Yet again fragmentation emerges as regards innovation performance and cybersecurity awareness. In addition, despite existing differences in capabilities, there is a divergence of views what is actually understood under a concept of cybersecurity. In the case of the NIS Directive, as

Figure 2. Enterprises which defined or reviewed their ICT security policy, 2015 (percentage of enterprises). Source: Eurostat 2015.



LT, TR : data unreliable

Ilves et all[15] note, "some governments, including Germany and the Netherlands, treat cybersecurity as a question of homeland security, while others, such as Latvia and Denmark, consider it a question of defence. Still other countries, including Finland and Italy, see cybersecurity as a matter of vcommerce and communications". These differences have contributed to the difficulties in cooperating on cybersecurity across the EU, as there is no strategic level forum to bring together the highest level cybersecurity decision makers and influence the dynamics of the negotiation process of this Directive.

4. Major Bones of Contention in the Negotiation Process

Considering major stumbling blocks in the negotiations between the Council of the EU and the European Parliament, one can observe that exactly the same issues/challenges emerge at a national level where the implementation of the NIS Directive process has started. In the overall implementation process, a significant role has been assigned to the European Union Agency for Network and Information Security (ENISA), for which the mandate[16] has already started to be reviewed.

15 | Ilves L. et al., *European Union and NATO Global Cybersecurity Challenges: A Way Forward*, "PRISM", Volume 6, No.2, 2016 [online] http://cco.ndu.edu/Publications/PRISM/PRISM-Volume-6-no-2/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/

16 | European Commission, *Evaluation of the European Union Agency for Network and Information Security (ENISA)*, 2016 [online] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf.

In the course of the negotiations, there were a number of moments when the finer details of the proposal happened to be discussed by the Council of the EU and the European Parliament, yet there was no common vision on the way forward with marked divisions existing between the Member States, the Council of the EU, and the European Parliament. As mentioned in the introduction to this article, it took three years for the process to complete, during which eight Presidencies of the Council of the EU and seven informal trilogues occurred before the NIS Directive was finally adopted.

Several factors contributed to the challenges in negotiating the NIS Directive. On the side of the Council of the EU, the Member States shared the view that cybersecurity was not just a matter of national security, or an economic or social issue, but a question that needed to be addressed across all areas of the policy, as already mentioned in the section above. However, what was discussed was the extent to which the NIS Directive would address economic, social, or national security issues. Such dispute, to a certain degree, resulted from the level of preparedness of the Member States, their innovation, and their historical legacy. At the beginning of 2015, it seemed there was no end in sight as there were significantly deep divisions regarding the scope of the Directive as well as the cooperation envisaged.

However, the negotiations went ahead and the need for a speedy adoption of the Directive was even given as a high priority by the European Council in the spring of 2015. Both the Council of the EU and the European Parliament redoubled their efforts to progress on the main contentious issues such as the extent to which the so-called Internet enablers could be included in the scope of the Directive, the scope and definition of these enablers, and the extent of cooperation that could be forged between the Member States in the future. Jurisdiction and enforcement as well as security requirements and incident notification were also to be addressed during the discussions, yet they played a secondary role compared to the first two main issues as agreement on these points would simplify further negotiations on the latter issues.

The delicate, substantial negotiations between all actors involved became much more interconnected. In order to strike a deal, a balance between agreements on the scope and level of cooperation needed to be found, not only between the Council of the EU and the European Parliament, but also among other fractions within each of these institutions.

4.1 Scope

There were several concerns related to the scope of the Directive. The initial proposal put forward by the European Commission addressed all operators within the scope in the same manner. This approach meant that classical critical infrastructures, such as power plants, financial services and the so-called Internet enablers like search engines and e-commerce platforms were identically addressed. This caused divisions both in the Council of the EU and the European Parliament as there was disagreement on whether these services should be given equal importance. The debate on the importance of such services to the internal market of the EU was quite polarized, contributing to the extended time required to develop a constructive way ahead.

> “ Since the EU apprehended the risk of fragmentation, particularly with regard to the identification of operators by the Member States, many supportive measures have been introduced.

Major concerns that were addressed regarding the scope included Member State disclosure of the list of sectors to be covered, identification of the operators in the indicated sectors, a unified approach of the EU to these inherently cross-border operators, and the essential difference in their criticality for the internal market vs. critical infrastructures to avoid the risk of fragmentation. The first concern that was addressed was the nature of criticality between the so-called Internet enablers and other critical infrastructures. Thus, the scope was divided and two different approaches were developed: one for operators of essential services (OESs), and the other for digital service providers (DSPs) who had previously been referred to as internet enablers. In comparison with the operators providing essential services, the approach to regulate digital service providers had been altered, so that a higher level of harmonisation could be created for those providers which were usually active in many Member States, addressing the need to have them regulated in an equal manner across the EU and also proportionate to the nature and degree of risk they may pose.

Since the EU apprehended the risk of fragmentation, particularly with regard to the identification of operators by the Member States, many supportive measures have been introduced as a result. These include the mechanism which stipulates that if an entity is active in multiple Member States, it is treated in the same manner across the entire EU; practical arrangements for the exchange of information between the Member States on the identified operators; a mechanism to ensure a harmonised approach to the identification of the operators such as guidelines, implementing acts, additional tasks for the Cooperation Group and the CSIRT network, assistance of ENISA and a robust review clause.

Operators of Essential Services (OESs)

Early on, the identification of OESs proved to be a challenge to negotiations as the identification of such operators was deemed to be a national security concern. Any attempts to have lists of the services or the operators were strongly opposed in the Council of the EU. Therefore, an urgent need emerges to understand the potential challenges the Member States might encounter when identifying the operators, since a detailed list of critical services is either not always present or is tailored per Member State. Fundamental criteria for the identification of critical assets might differ across the EU; that is why there is a need for effective collaboration between the public and the private sector to identify and protect critical infrastructures, as one of the studies[17] of ENISA indicates.

Consequently, in an attempt to reach a compromise on the other issues, a solution was proposed that the European Commission would receive lists of OES services included in the national lists for the purpose of reviewing the Directive and the consistency of application of the Directive across the EU. Additional safeguards to ensure the harmonisation of equal identification of OES across the EU included informing the European Commission of "the number of operators of essential services identified for each sector referred to in Annex II and an indication of their importance in relation to that sector; [and] thresholds, where they exist, to determine the relevant supply level by reference to the number of users relying on that service [...]"[18]. Identification of the digital service providers also proved to be a challenge; however, this issue was solved by defining the DSPs for the purpose of the Directive. The first report assessing the implementation of the Directive shall be submitted by 2021.

17 | ENISA, *Methodologies for the identification of Critical Information Infrastructure assets and services*, 2015 [online] https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis.

18 | European Commission, *Directive 2016/1148 Of The European Parliament And Of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, 2016 [online] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive; Article 5, para7c and d. [online] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

Digital Service Providers (DSPs)

The final unsettled point of disagreement on the scope was the list of DSPs. Originally, the list contained e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, and application stores. It was however the European Parliament which from the onset postulated for the exclusion of the information society services; but a compromise needed to be found as a blocking majority in the Council of the EU emerged on this particular issue. Yet when a separate approach to and an agreement on cooperation was reached, a compromise to only include online marketplaces, search engines, and cloud computing services was relatively easily agreed upon in the final stages of negotiations.

> “ The final unsettled point of disagreement on the scope was the list of DSPs.

Nonetheless, there were a number of issues to be resolved in the process of the negotiations which referred to the lack of legal definitions of the so-called Internet enablers in the original proposal of the European Commission; uncertainty on the questions of territoriality and enforcement, taking intrinsically cross-border nature of many of the services concerned. Throughout the negotiations, the parties maintained that the lack of definitions might pose a challenge of setting a clear boundary between the scope of the NIS Directive and the Framework Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, where electronic communication service providers are already subject to security requirements and incident notification under Article 13a. It has been argued that the taxonomy of the so-called OTTs (over-the-top) services should be introduced in the sectoral act i.e. the Framework Directive, Audio-visual Media Services Directive (AVMSD), or e-Commerce Directive, when reviewed. The acquis only provided for a definition of an online marketplace. Additionally, the existence of multiple reporting mechanisms, either under the indicated Framework Directive, the general data protection regulation, or the e-privacy Directive, proved to be another challenge. As a way out, a separate clause in Article 1(7) on the application of sector-specific Union legal acts was drawn up to solve the issue in question. Some Member States argued that, for the reasons mentioned above, digital service providers should be included into the scope after the revision of the Directive takes place. It remains to be seen how the application of these provisions will relate to the said review of the Framework Directive, which under the heading the European Electronic Communications Code was published in September 2016.

4.2 Cooperation

As far as cooperation in the negotiations is concerned, all sides agreed that cooperation at the EU level on NIS matters with designated competent authorities in each Member State of the EU was beneficial and necessary, both at the strategic and operational level. The levels of compulsory cooperation became and remained a contentious issue throughout the negotiations for several reasons.

> “ All sides agreed that cooperation at the EU level on NIS matters with designated competent authorities in each Member State was beneficial and necessary, both at the strategic and operational level.

As in any other cybersecurity debate, trust and information sharing were the key points of discussion on cooperation. Debates on formalised

cooperation concluded that trust could not be mandated; yet trust could be built only if all actors had the opportunity to engage with each other. Also information sharing made the negotiations more difficult as national security issues clouded the debates with some Member States being open to higher levels of information sharing and others being more guarded, especially with regard to not only national security considerations, but law enforcement and investigation issues as well. Such divisions may have stemmed from different levels of capabilities and preparedness in the Member States, which has been outlined in section 3.

Once it was established that there would be two separate cooperation groups, the details of the functioning of these groups were heavily scrutinised. The European Parliament emphasized the need for a clear timeline and an effective governance structure for the operation of these two bodies as well as proper reporting and review mechanisms. While there was no disagreement in the Council of the EU in principle, several points of contention arose out of these issues. To provide for an effective governance structure, a secretariat needed to be formed for the groups, although different modes of involvement had been envisaged for the European Commission, ENISA and CERT-EU to communicate. The need for reporting and review was not dismissed; however, the challenge lay in not creating administrative burden that would weigh the groups down with administrative work when the purpose of setting up these groups was information sharing and building trust. Compromises had to be made to find a balanced solution: The Cooperation Group includes ENISA and the European Commission, the latter being responsible for the secretariat; while the CSIRT network is composed among others of the CERT EU, ENISA as secretariat and the Commission as observer. In addition, a review process was developed, according to which the CSIRT network reports periodically to the Cooperation Group, which, in turn, prepares an overall report on cooperation.

The extent of cooperation has been detailed in the Directive; however, due to the need to find a compromise and a balanced package between cooperation and scope, the mandatory nature of such cooperation is very limited. The Cooperation Group will not only exchange best practices, relevant information, and experience, but will also discuss various issues related to the Directive and its implementation as well as examine the work of the CSIRT network. Early requests by the European Parliament regarding a possible new and costly secure information-sharing system, early warning and response, and a Union NIS cooperation plan were withdrawn in the course of negotiations since a compromise needed to come as a package.

Conclusion

This article attempted to shed light in the dynamics of the negotiations on the NIS Directive and the hurdles encountered in the course of the lengthy and obscure legislative process. While the directive has been adopted, there are still challenges that will be faced during the implementation phase, as the same hurdles faced in negotiations may still lead to incoherence of the approach by each Member State, if the Directive fails to be implemented uniformly. As it has been noted beforehand, fragmentation in the Single Market is the Emperor's not so new clothes and might not be preventable. However, the general barriers of regulatory heterogeneity in the Single Market have been identified and some recommendations have already been provided. The said recommendations can also be applied to the NIS Directive as well[19]. On the better regulation front, in the Better Regulation agenda[20], the European Commission has hardwired its commitment to evidence-based

19 | European Parliament, *The Cost of non-Europe in the Single Market. Cecchini revisited*, 2014 [online] http://www.europarl.europa.eu/RegData/etudes/STUD/2014/510981/EPRS_STU(2014)510981_REV1_EN.pdf See in particular the conclusions listed in the executive summary, pp. 10-11.

20 | European Commission, *Better regulation for better result – an EU agenda*, 2015 [online] http://ec.europa.eu/info/files/better-regulation-better-results-eu-agenda-0_en.

policy-making pronouncing that "evidence is needed both to evaluate existing interventions and to substantiate new ones". Among other commitments, the European Commission vowed to: consult more, listen better; what is doing, and why (explaining how better regulation principles have been applied, why the initiative is needed and why it is the best tool for the EU to use), provide better regulation as a balanced agenda (as better regulation is not about favouring certain policies or objectives over others) and refresh existing legislation (looking at the cost and benefits while conducting assessments and evaluations over a policy's lifetime). In May 2016, Ministers emphasized in a joint letter[21] "the importance of taking an evidence-based approached, basing new legislative proposals on better regulation principles and especially conducting sound and thorough impact assessments to ensure a balanced and proportional level of regulation" in order to establish a simple, stable and transparent regulatory environment.

But such commitments might have actually clashed with the applied practice of the European Commission. In the ruling of the European Ombudsman on the Connected Continent package[22], the EU watchdog – in reply to the European Competitive Telecommunications Association's (ECTA's) complaint of September 2013 – pronounced that European Commission services had not followed general principles and the minimum standards of public consultation specified in its own rule. In addition, it remained unclear whether the urgency claimed by the European Commission reflected only the European Commission's own assessment. As a result of the rushed process, the original proposal – in the course of the negotiations – has been slimmed down to the topics of open internet, roaming and a skimpy part on end-user rights. However, it appears that the promised "abolition" of roaming as of 2017 might have sailed into rough seas. The roaming regulation foresees the possibility for an operator to apply a fair use policy. However, at the time of writing this article in September 2016, following a public outcry, the Commission services have withdrawn the draft of the implementing measures and are working on a new version on the instruction of President Juncker[23].

Drawing on its experience in its own initiative report Towards a Digital Single Market Act[24], the European Parliament called the European Commission to fight legal fragmentation by significantly increasing the coordination of its various DGs, while drafting new regulation and strongly encouraging the Member States to ensure that implementation of the regulation remains coherent.

In the field of cybersecurity, fragmentation is still present but improvement is noticeable and possible through the implementation of the NIS Directive, despite the differences between Member States as outlined in the previous sections. The European Commission released on 5 July 2016 a new communication[25] on improving cyber resilience. While it has indicated that the communication "addresses additional market-oriented policy

21 | Joint letter from Belgium, Bulgaria, Czech Republic, Denmark, Estonia, Finland, Ireland, Latvia, Lithuania, Luxembourg, Poland, Slovenia, Sweden and United Kingdom in preparation of the Transport, Telecommunications and Energy and Competitiveness, Council meetings, 26 May 2016.

22 | European Ombudsman, *Decision in case 904/2014/OV on Regulation of the European Commission's public consultation prior to its legislative proposal for a Regulation Parliament and of the Council laying down measures concerning the European single market for electronic communications*, 2015 [online] http://www.ombudsman.europa.eu/en/cases/decision.faces/bg/60965/html.

23 | Commission implementing the EU Regulation laying down detailed rules on the application of fair use policy and on the methodology for assessing the sustainability of the abolition of retail roaming surcharges and on the application to be submitted by a roaming provider for the purposes of that assessment [online] http://ec.europa.eu/info/law/better-regulation/initiatives/ares20164977189_en.

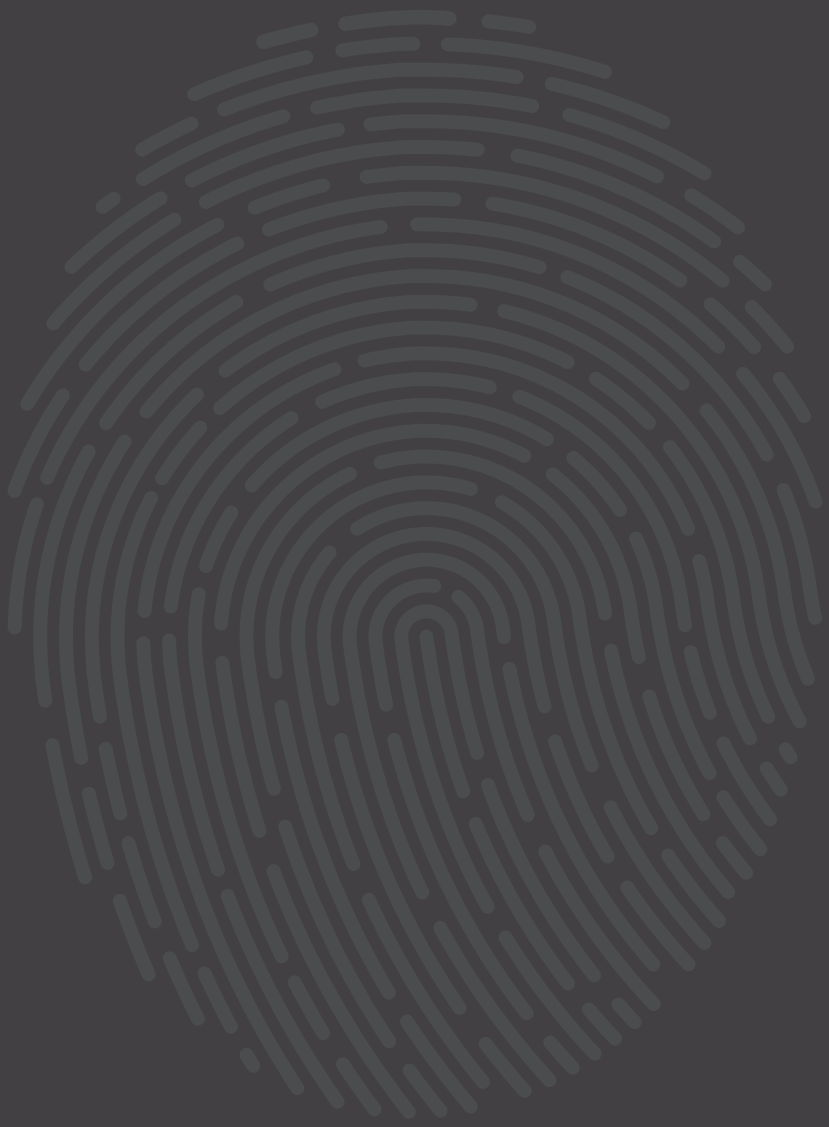
24 | European Parliament, *Towards a Digital Single Market Act*, 2016 [online] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2015-0371+0+DOC+XML+V0//EN.

25 | European Commission, *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*, 2016 [online] https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and.

measures to boost industrial capabilities in Europe"[26], the communication does address cooperation, an issue that during the negotiations on the Directive proved to have very little to do with market-oriented policy measures, but rather issues of national security. The European Commission has always supported more strengthened measures on cooperation and have reintroduced some measures that were cut from the directive into the communication. At the time of publication, there is however limited enthusiasm among Member States on the communication, as the full national resources of the Member States are completely devoted to the implementation of the NIS directive. In addition, as the study of the European Parliament noted: "understanding how coordination and cooperation is achieved in the European cybersecurity policy puzzle is very complex. No one currently has a clear understanding of how all the different pieces fit together", which does not really contribute to the process of implementation of both the cybersecurity policy and related legislation. In conclusion, the work ahead on cybersecurity does need to continue and new initiatives may be necessary in order to address new issues. However, the first and foremost priority for the European Union now is the implementation of the NIS Directive. Undoubtedly, it will be a tedious task, requiring consultations among the Member States. However, this is what over the course of many years the Member States of the European Union have decided upon and now a long, meticulous, and coordinated process will continue that will not have the ups and downs or screeching halts experienced during the negotiations. Instead, the implementation will be a bureaucratic, and systematic process to consistently and effectively increase the security of network and information of the European Union over time. ■

26 | Ibid.

CISCOSEC



NOVEMBER 15-16, 2016

Double Tree by Hilton

ul. Skalnicowa 21, 04-797 Warszawa

www.ciscosec.pl

ANALYSIS

TOP FIVE SECURITY THREATS FACING YOUR BUSINESS AND HOW TO RESPOND

ANN JOHNSON

Ann Johnson leads the Enterprise Cybersecurity Group within the Enterprise & Partner Group at Microsoft. ECG's mission is to empower enterprises to confidently move to the cloud and modernize their platforms. Before joining Microsoft, Ann was CEO at Boundless, an open source geospatial software and services provider. Ann is a recognized cybersecurity industry leader with a proven track record for building and leading high-performing global enterprise software operations. Ann is a graduate of Weber State University in Utah where she completed a dual major in political science and communications.

Headlines highlighting how vulnerable we are to cyberthreats are now all too commonplace. The statistics on security events and successful network breaches continue a trend that favours attackers. These bad actors are getting faster at network compromise and data theft while their dwell times inside networks have increased to over 200 days according to most of the major annual cybersecurity reports. The result of these voluminous and persistent threats has been hundreds of millions of dollars in lost business alone without counting the long-term costs of diminished customer and citizen confidence.

Still organizations may face even greater risks as they try to fend off sophisticated attackers against a backdrop of an ever expanding network footprint. The new network now includes myriads of personal devices, virtualized workloads, and sensors that represent rapidly increasing points of connectivity as well as potential compromise.

When considering these trends, it is clear that the traditional means of protecting organisations are not as effective as they once were. Static access controls like firewalls and intrusion prevention systems placed at network ingress and egress points are being easily evaded by attackers because the communications paths in and out of networks are too complex and dynamic. Also broad use of personal devices inside corporate networks has dissolved what used to be a hardened network boundary. We no longer conduct business within a perimeter of highly controlled, corporate-issued end-user devices that gain access only under the strictest of authentication and authorization controls. Instead, the modern enterprise enables dynamic communities of employees, contractors, business partners, and customers as well as their data and applications, all connected by an agile digital fabric that is optimized for sharing and collaboration.

In today's networks then, we have to consider that identity is the new perimeter to be protected. Identity in this case does not mean only the device and its physical location but also the data, applications, and user information it contains. Given that 60% of all breaches still originate at an end point compromised through a phishing scam or social engineering attack, it is no wonder that a risk mitigation strategy with identity at its centre is top of mind for many business and technology leaders.

In fact, cybersecurity is a boardroom level agenda item today. Business leaders want to ensure that they have in place the investments necessary to protect intellectual property and customer data, keeping their businesses out of the headlines that damage reputation and affect profitability. CIOs and CISOs feel caught between seemingly opposing goals of enabling digital transformation while protecting data and intellectual property at all times. These are concerns they share with their teams in IT and operations who feel equally burdened to balance performance and accessibility with rightful and appropriate resource use. Cybersecurity, as we have all come to understand,

can be either a critical barrier or a key enabler to an organisation's ability to be productive. Current top of mind concerns for protecting the modern enterprise coalesce around 5 key areas: infrastructure, SaaS, devices, identity, and response.

1. Infrastructure

The public cloud offers unlimited potential for scaling business. On-demand compute and storage is only a small portion of the benefits of a highly agile IT environment. Easy access to applications, services, and development environments promises to redefine business agility. Naturally, more and more organisations are taking critical workloads to the public cloud. Still, the migration to an environment that is provisioned and managed by a non-organisational stakeholder creates new security challenges. So the top of mind question is: "*How do I secure my cloud resources?*"

> "Cloud users should also be familiar with the security technologies offered by their provider whether native or through partnership.

Going to the cloud does not mean relinquishing security control or accepting a security posture that is less secure for cloud-hosted workloads relative to premised ones. In fact, the selection of a cloud provider can mean having access to the very latest in security technologies, even more granular control, and faster response than is possible with security in traditional networks. As a first step, security stakeholders need to understand how sensitive and compliance intense their cloud-hosted workloads and data are. They should then opt for access controls that limit use to only that which is business appropriate and emulate those access policies already in place for premised workloads. Enrolling in cloud workload access monitoring will also ensure that any events which are a deviation from desired security policies can be flagged as indicators of possible compromise. Cloud users should also be familiar with the security technologies offered by their provider whether native or through partnership. This gives cloud users options for implementing the kind of multi-tiered security architecture required to ensure least privileged access, inspect content, and respond to potential threats.

Key takeaways

- Monitor workload access and security policies in place
- Identify deviations from security policies and indicators of possible compromise
- Deploy new security controls appropriate for your cloud environment

2. SaaS

Whether a business is hosting critical workloads in the public cloud or not, its employees are surely using applications there. The convenience and ubiquity of these applications means broad user adoption for the ease of information sharing and collaboration they enable. As a result, important, security and compliance intense data maybe making its way to the public cloud without the security stakeholder's knowledge. The question from businesses then is: "*How do I protect my corporate data?*"

Organisations want to make sure their employees are as productive as they can be. To that end, many are allowing them to bring their own devices and even their own applications into the network. This agility comes with some added security risk. Fortunately, there are ways to mitigate it. Ultimately, the goal is to derive all of the benefits these SaaS applications offer without violating company use and compliance policies for data sharing and storage. Additionally, firms must ensure that employees' use of SaaS applications does not unwittingly enable data exfiltration by bad actors. Limiting the risk comes down to enacting a few of

the basics that ensure safe use. For starters, there is a need to identify which SaaS applications are in use in the network and whether they are in line with the company policy or on a safe list. Granular access rights management will limit the use of even the safe applications to those persons who have a business need for them. Where possible, policies should be in place that require data to be encrypted when at rest, especially if it is being stored in the cloud. Having the ability to periodically update the safe lists of applications and monitor all use, can potentially alert security administrators when those applications which are unsanctioned appear among an organisation's communications. With these types of facilities in place stakeholders may be promptly alerted to unsanctioned application use. At times, unwanted application use will be detected. This is the time to block those applications, modify, or deprecate privileges allowing access to them and, as a further precaution, remotely wipe or delete data stored through the use of those applications.

Key takeaways

- Apply rights management, identify unsanctioned applications, contain, classify, and encrypt data
- Be notified of unauthorized data access or attempts
- Block suspicious applications, revoke unauthorized access, and remotely wipe company data

3. Devices

Smartphones, tablets, self-sourced laptops, these are the new network perimeter and, at times, its weakest links. Whether owned by the organisation or not, they most certainly contain business valuable data that is at high risk. Because mobile devices often connect from public networks and may not have the most up to date protections, these end points are popular targets for the installation of botnets or malware. The use of personally sourced devices is a new and seemingly permanent reality prompting organisations to broadly ask "*How do I keep company information secure?*"

> "Today's security administrators have to accommodate a heterogeneous end-user device environment.

Many years ago, risk from mobile devices was ameliorated by installed agents and thick clients that provided security controls right on the device itself in a centralized way. Today, with employee self-sourced devices, the installation of such clients is not always feasible. Still, today's security administrators have to accommodate a heterogeneous end-user device environment comprised of various form factors and OSes, while applying consistent and organisationally sanctioned controls to all of them. A cloud-based approach can provide a lot of flexibility and control here. From the cloud, end point connectivity to network resources can be centrally managed through security policies that restrict where devices can go, based on their security posture, installed protections, or location-based access rights. The command of devices from a central location ensures not only consistent policy enforcement but automation so that when anomalous device behaviours or connection patterns are detected, centralized command can restrict access, quarantine the affected device, and even wipe it clean so that the threat is fully contained.

Key takeaways

- Manage company and personal devices to classify and encrypt data to ensure compliance
- Automatically identify compromised or questionable end points
- Quickly respond to quarantine, wipe and remediate compromised devices

4. Identity

Despite all of the investments organisations make in security and threat mitigation, identity will be compromised. The latest data tells us that way too many of us click on links and attachments that we should not. From that point on, the bad actor has gained a foothold in the network and may set about moving laterally, looking for sensitive information to steal while impersonating the legitimate user. This common scenario is what makes many businesses ask: "*How can I ensure identity protection?*"

> Implementing multi-factor authentication broadly for all applications and services is a good starting point.

All of the major cybersecurity reports and indices point to this as the most common component of a data breach – the stolen identity. A security strategy for any organisation or business needs to have this as a central tenet. The protection and management of credentials that give resource access to customers, employees, partners, and administrators is foundational to a sound security practice. Implementing multi-factor authentication broadly for all applications and services is a good starting point. It should nevertheless be complemented by facilities for monitoring authentication and authorization events not only for users, but also, and especially, for privileged users and administrators. This type of monitoring offers the best opportunity to identify attempts by attackers trying to move laterally through privilege escalation. Once flagged as suspicious and anomalous, optional automated response can ensure that access requirements are elevated on the fly and privilege escalation requests are verified as legitimate.

Key takeaways

- Augment passwords with additional authentication layers
- Identify breaches early through proactive notification of suspicious behaviour
- Automatically elevate access requirements based on your policy and provide risk-based conditional access

5. Response

Each year organisations are subjected to tens of thousands of security events, making the business of protecting critical assets continuous. Given that threat dwell times are 200 plus days, bad actors have ample opportunity to move "low and slow" throughout networks after the initial compromise. Naturally, security administrators and stakeholders are left to ask: "*How can I better respond to ongoing threats?*"

> Remains at risk so the process of protecting, detecting, and responding to a breach is a continuous one.

The potency and frequency of today's cyberthreats requires a security strategy built on the assumption of compromise. A network or device may not be breached today, but remains at risk so the process of protecting, detecting, and responding to a breach is a continuous one. The data that is being exchanged by end points and shuttled among data centres and hybrid clouds contains a lot of information about the security state of those end points and resources. The key to unlocking that intelligence is analytics and specifically the type of analytics that is made possible through machine learning. Having the ability to monitor large amounts of traffic and information in a continuous fashion and unearth anomalous behaviour is and will be key to shortening the time to detection of a breach or compromise. Behavioural analytics

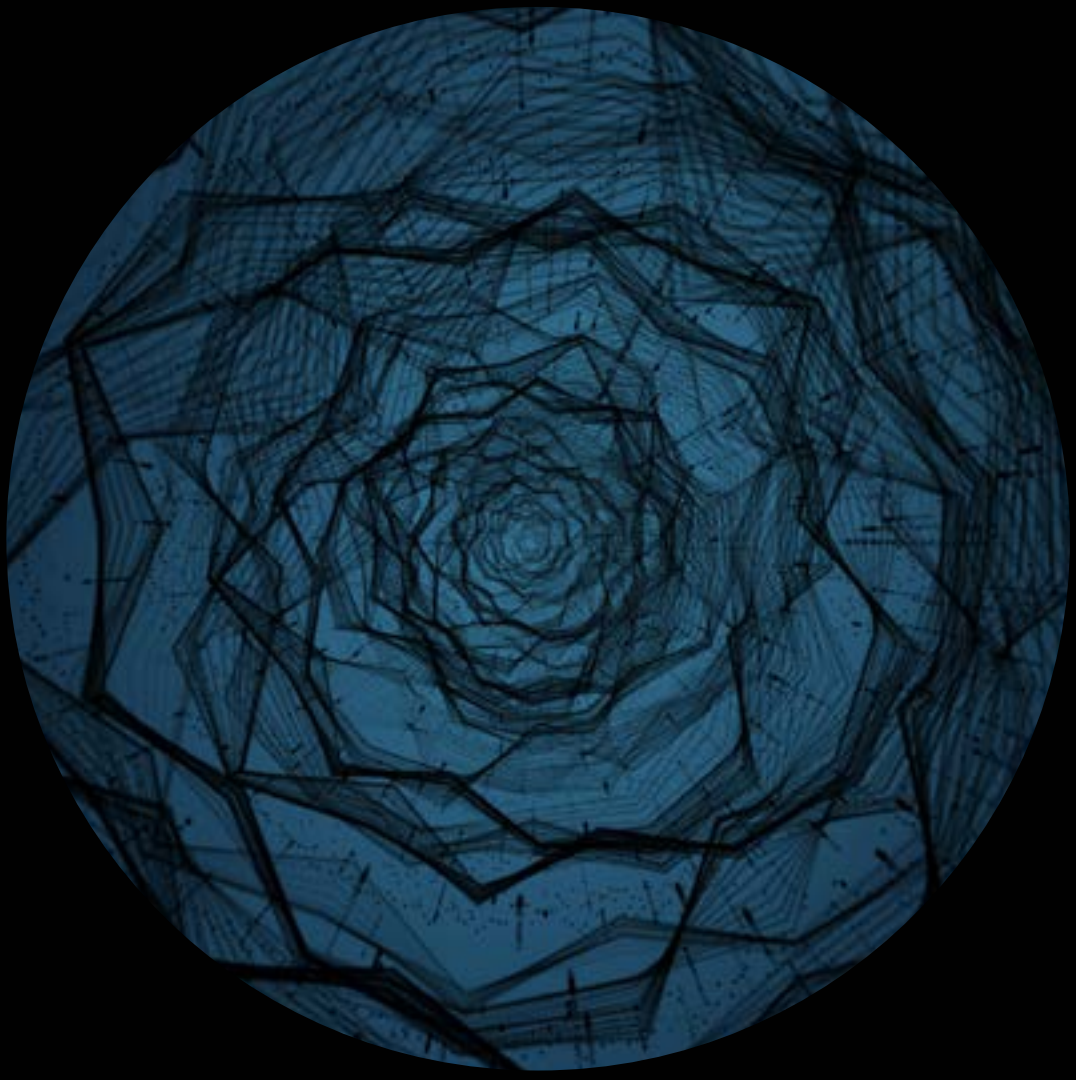
not only tells us what is out of the norm or unwarranted behaviour, but also informs of good and desired connectivity. By understanding both anomalous and appropriate traffic patterns, organisations can fine-tune access controls that are just right for enabling business yet limiting risk. Further, with continuous analytics, the process of determining the right access controls for the environment at a given time can be as dynamic and responsive as users' access needs.

Key takeaways

- Use analysis tools to monitor traffic and search for anomalies
- Use learnings from behavioural analysis to build a map of entity interactions
- Practise just-in-time and just enough access control

In summary, security threats may be common to businesses and organisations of all types, but the way they are addressed can vary greatly. In the modern enterprise driven by mobility and cloud, architecting for security represents an opportunity for unprecedented agility. With a strategy built on identity as the new perimeter and access to continuous processes to protect, detect, and respond to threats, a business can be as secure as it is productive. ■

Deloitte.



Secure.
Vigilant.
Resilient.

www.deloitte.com/pl/cyber

ANALYSIS

CYBERSECURITY OF INDUSTRIAL CONTROL SYSTEMS: SOME ASPECTS OF CURRENT PROBLEMS

ANDRZEJ KOZAK
Dr Kozak is an executive arm of the Polish government to ensure the legal conformity in The Office of Technical Inspection. He was responsible for creating a team of specialists to process safety analysis. Currently he holds an advisory position to the President of the Office and he specializes in cybersecurity of industrial control systems. He also is a senior lecturer at the Technical University of Lodz at Department of Process Safety for the postgraduate students. He graduated from Chemical and Process Engineering Program at the Cracow University of Technology. He developed further interest in the process engineering, performed a research and achieved a PhD degree from the Polish Academy of Sciences – Institute of Chemical Engineering. Dr Kozak has more than 35 years' experience in safety process industry and safety management.

With the dynamic expansion of a digital world (the internet of things, digital control systems, etc.), wireless connectivity and digital communication have a great influence on our lives, national economies, and a social sense of security. But this expansion creates a paradox: although our cyberspace is a very efficient and effective operation, it dramatically and rapidly decreases the social feeling of cybersecurity.

> "Cyberattacks on the manufacturing industry could generate problems with the Industry 4.0 - the project of the 4th industrial revolution.

Cyberattacks on the manufacturing industry could generate problems with the Industry 4.0 – the project of the 4th industrial revolution. The last cyberattacks against various industries have shown that the threat of cyberattacks against critical infrastructure, be they of terrorist or military type, are very realistic.

Differences between IT (Information Technology) and ICS (Industrial Control System)

In order to establish an effective cybersecurity programme incorporating the Industrial Control System (ICS), it is very important to know the differences between IT (the business side) and ICS (the operational side) as illustrated in Table 1. The term "Industrial Control System" denotes a system and application that is generally implemented and managed by specialists outside the business IT function such as production, engineering, and maintenance – their primary goal is production, not security. The ICS environment has inherent security challenges emanating from different IT technologies and different

security strategies, which are further aggravated by old ICS systems that may have no connection to the Internet.
The IT system of a plant is a business system whose primary cybersecurity goal is to protect data (confidentiality), while the main cybersecurity objective of ICS is to provide technology and ensure availability of plant. Protection of information is important but a slump in production means lower income. The main differences between the business/corporate IT and the industrial control system (ICS) are summarized in Table 1[1].

Table 1. The most essential differences between ICS and corporate IT systems.

	ICS	IT
Availability of provided services	24 hours by 7 days by 365 days / year	Restarted when needed
Latency	Real-time requirements	Varying response times are accepted
Depreciation	10 to 25 years	3 to 5 years maximum
Passwords	Usually hard wired in legacy ICS; group passwords never changed.	Regularly changed

There are also differences in the management of IT and ICS resources. They are usually allocated to different departments: IT resources are typically managed by the IT department that employs IT specialists, while the ICS resources are assigned to the department of production and/or technology, commonly managed by the automation engineers. This may cause particular difficulties with the mutual understanding of the needs, expectations, and necessary action for establishing proper and effective cybersecurity procedures for industrial control system.

Managing Cybersecurity Risk of Industrial Cyberspace

Currently, digital control systems are divided into the following groups:

1. Computer systems, such as DCS, SCADA, etc. industrial control systems
2. Non-computer systems (embedded computer systems) for drives e.g. on-board computers in vehicles
3. Non-computer systems in intelligent (smart) buildings – like Heating Ventilating Air Conditioning (HVAC), lifts control, fire detection and firefighting systems, etc. Interrelation between the systems is illustrated in Figure 1.

Figure 1 also shows the areas that will be included in Industry 4.0. The project Industry 4.0 includes: Internet of Things, Diagnostics and Maintenance. In view of a high degree of network connections, Industry 4.0 may be particularly vulnerable to network hacks and cyberattacks. The Industrial Internet of Things (IIoT) hinges upon effective cybersecurity. Cybersecurity of industrial control systems "deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control And Data Acquisition (SCADA) systems, Distributed Control Systems (DCS),

1 | See more details here: Luiijf E. and Jan te Paske B., *Cyber Security of Industrial Control Systems*, GCCS, March 2015.

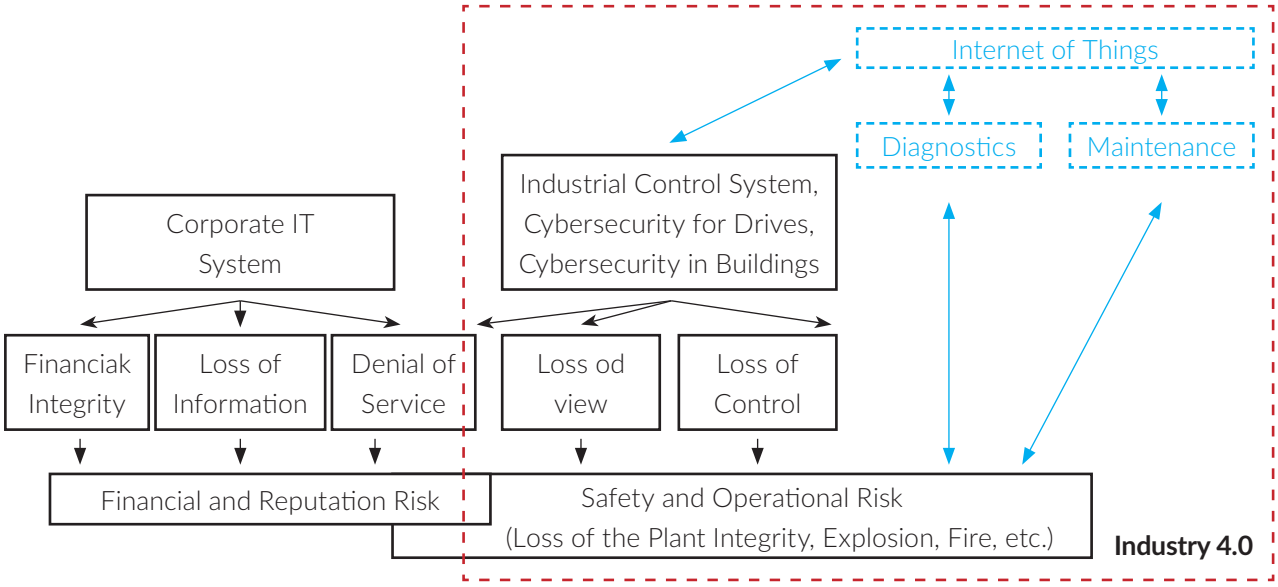


Figure 1. The relationship between IT systems, digital control systems and the expected Industry 4.0 impact zone (based on an IET study[2]).

Process Control Systems (PCS), Industrial Control Systems (ICS); critical business systems; and other sensitive computerized systems"[3].
A cyberattack on an Industrial Control System is usually conducted in the following two ways:

1. The attack on the business/corporate IT system with the purpose of achieving a "propagation effect", i.e. by dissemination of malicious software into the IT system and finding ways to enter into the Industrial Control System.
2. After finding ways to "invade" the control system, a phase of misinformation of the operator follows (disinformation effect). That is, information which is observed by the operator on the process monitor is not related to the actual processed data. The final phase of these operations is the loss of physical assets, fire, explosion, accumulation of hazardous substances, etc. The interaction between the effect of propagation in IT systems and the effect of misinformation in ICS are shown in Figure 2.

Cyberattacks on industrial installations are almost always compound of a sequence of events to recognize both the technological and social security ways. As far as social security is concerned, attackers tend to search through social networking sites: maybe there is someone who boasts about what they do in the factory, maybe someone is looking to solve a problem with a control range, maybe someone will be careless enough and open an e-mail sent to him from an unknown address. In about 80% of all successful cyberattacks on the manufacturing industry, the attacker had an informant inside the plant. However, the source of information was often unaware of the impact of their activities.

> "Proper enterprise information architecture makes it more resistant to carry out an effective cyberattack.

2 | IET (The Institution of Engineering and Technology), *Resilience and Cyber Security of Technology in the Built Environment*, IET publications, 2013.
3 | US Department of Homeland Security, *Risk-Based Performance Standards Guidance. Chemical Facility Anti-Terrorism Standards*, May 2009.

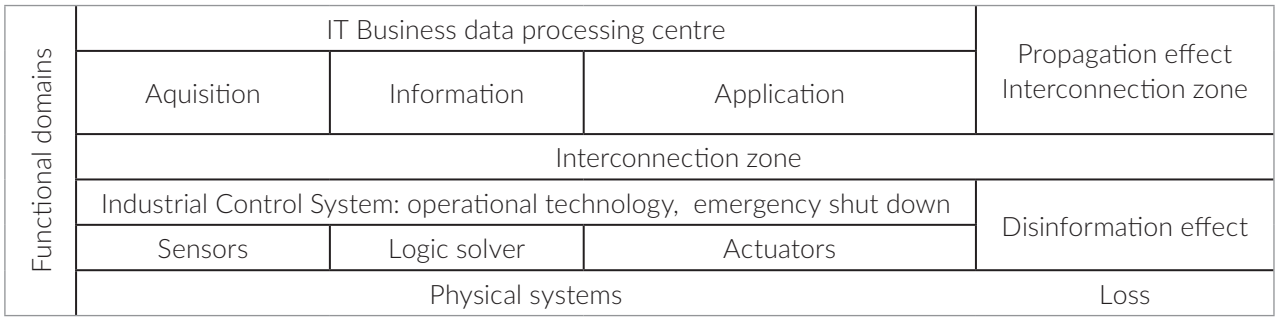


Figure 2. Propagation and disinformation effects acting on industrial cyberspace.

Proper enterprise information architecture, i.e. a security system that encompasses organization, infrastructure and personnel, makes it more resistant to carry out an effective cyberattack4. Risk analysis allows security issues to be evaluated and adequate security tools to be selected and implemented. Cyberattacks on industrial control systems are often carried out using smartphones. When plant management staff has access to them via mobile devices which are poorly protected, it is possible to attack ICS of the plant according to the following scenario5: through an earlier infected smartphone, a hacker defeats the firewall and gains access to a company workstation. The workstation typically identifies the hacker as a registered user and allows him to exchange information. The hacker gains access to control systems as well as collects and sends data to ICS. From this point onwards, the hacker has unfettered access to critical data and may cause damage to the plant system. Non-computer systems may also be subject to a cyberattack. An embedded operating system is an operating system for embedded computer systems (non-computer system). These operating systems are designed to be compact, efficient at resource usage, and reliable, forsaking many functions that non-embedded computer operating systems provide, and which may not be used by the specialized applications they run. They are frequently also referred to as real-time operating systems. Embedded systems are used to control various elements of the vehicle (engine control, traction control of the vehicle, braking system, etc.). The system used in vehicles was created in the early 1990s of the last century, when the phenomenon of hacking did not exist. Currently, digital systems in vehicles are prone to dangerous hacker attacks6,7. The parts of the cars that are most commonly targeted by hackers are listed in Table 2.

Table 2. Most frequently hacked parts in modern cars.

ECM	Engine Control Module
EBCM	Electronic Brake Control Module
TCM	Transmission Control Module
BCM	Body Control Module
Telematics	Enables remote data communication with the vehicle via cellular link
RCDLR	Remote Control Door Lock Receiver
HVAC	Heating, Venting, Air Conditioning
SDM	Inflatable Restraint Sensing and Diagnostic Module: controls airbags and seat belt pretensioners
IPC / DIC	Instrument Panel Cluster / Driver Information Center: displays information to the driver about speed, fuel level, and various alerts
Radio	Radio
TDM	Theft Deterrent Module: prevents vehicle from starting without a legitimate key
RCDLR	Remote Control Door Lock Receiver

4 | Pacyna P. et al., *Metodyka Ochrony Teleinformatycznych Struktur Krytycznych, PWN 2013* (Polish edition only).

5 | See the diagram of this procedure and more detailed information here: Control Eng., Polska number 4/120, July/August 2016, p. 80.

6 | US Government Accountability Office, *Vehicle cybersecurity*, Report to Congressional Requesters, March 2016.

7 | McAfee, *Automotive Security Best Practices. Recommendations for security and privacy in the era of the next-generation car*, White Paper, Intel Security, 2015, available at http://www.mcafee.com/de/resources/white-papers/wp-automotive-security.pdf

Nowadays, more and more cars are equipped with intelligent digital modules, and their functions range from simple music playing to complex semi-automated driving. Modern vehicles create a specific automotive ecosystem that can be prone to an attack due to the following elements[8]:

1. Increased penetration of connected vehicles
2. Standardised vehicle platforms using the same electronic backbone
3. Support for external connection devices
4. Lack of hardware and software security elements used in vehicles

So, a common phrase to "remember to lock your car" may no longer be a sufficient piece of advice. Similar problems related to cybersecurity exist in smart buildings. Buildings are increasingly IIoT-enabled (Industrial Internet of Things) and made functional by two different technologies: an operational technology (OT) and an information technology (IT)[9,10]. Moreover, the cyberspace of intelligent buildings has an open access to many operators and services providers. Some critical parts of the intelligent building can be particularly vulnerable to cyberattack – e.g. fire protection system, elevators, heating and ventilation, as well as access control to different areas of the building, alarm systems and security, CCTV (Closed Circuit Television – industrial television), etc. Five best practices to improve Building Management Systems' (BMS) cybersecurity are reported as "5 x management"[11]:

1. Password management
2. Network management
3. User management
4. Software management
5. Vulnerability management

For more detailed information on cybersecurity of buildings specified in the standard of the Centre for the Protection of National Infrastructure, please see "Resilience and Cyber Security of Technology in the Built Environment"[12].

Risk analysis in an ICS cycle

The suggested risk analysis of each system (computer and non-computer alike) should give full answers to the below eight questions[13]:

a. What security measures are in operation?
b. What are the current and planned network structures?
c. What are the information and control flows?
d. What is the probability of different types of attack?
e. What are the consequences of the attack?
f. What plans are in place for regular security audits?
g. What training for personnel and partners is available?
h. h. What incident response procedures are in place?

As a standard measurement, a cyber risk metric must be clearly defined and known before risk analysis is done. There are three types of cyber risk metrics:

1. Organizational: cybersecurity policies, access control, personnel security, unique accounts, etc.
2. Operational: awareness and training, cybersecurity controls, monitoring, response, and reporting
3. Technical: disaster recovery and business

8 | Thoppil T. and Bittersohl C., *Automotive Cyber Security. Developing a thriving security ecosystem within automotive organizations*, White Paper, P3 North America Inc, n.c.

9 | TU-Automotive, *TU-Automotive Hack and Threats Report 2016*, 2016, available at www.tu-auto.com/cyber-security-europe.

10 | Khaund K., *Cybersecurity in Smart Buildings*, Frost & Sullivan Report, September 2015.

11 | Williamson J. and Strass G., *Five Best Practices to Improve Buildings Management Systems Cybersecurity*, Schneider Electric White Paper, 2014.

12 | IET, *Resilience and Cyber Security of Technology in the Built Environment*, IET Standards and Centre for the Protection of National Infrastructure publication.

13 | Control Engineering, *The cyber security checklist*, 11 February 2014, available at http://www.controlengeurope.com/article/69753/The-cyber-security-checklist.aspx

continuity, configuration management, cyber asset identification, audits, etc.

Cyber metrics and risk analysis methodology are of fundamental importance for a facility risk matrix, individual for each facility. A risk matrix defines risk categories as a function of a cyber risk and possible losses provoked by the cyberattack (see Figure 3). In this, the risk matrix combines the likelihood of possible scenarios to occur as a consequence of a cyberattack on an industrial control system and the severity of a cyberattack. The cyber risk matrix should to be unique to each plant and must be approved by the corporate board of directors.

Pre-requisites increasing the probability of a successful cyberattack:

1. Vulnerabilities or weaknesses must exist in the defended system.
2. The attacker must have sufficient resources to find and exploit the vulnerabilities or weaknesses of the defended system. This is referred to as the “capability”.
3. The attacker has to believe that the attack will bring them substantial benefits.
4. Expected benefits are motivational drivers.

Whilst condition 1 relies completely on the defender, conditions 2, 3, and 4 hinge upon the attacker. Although the defender may provoke an attack, they must take into account the fact that there may be more than one attacker at a time.

Conclusions

Safety and security are not expenses, they are pure profits. Several points are worth mentioning in conclusion to this analysis:

1. The balance between transparent user access and maximum security of the other side has to be clearly defined.
2. Cyberattack scenarios have to be sorted by risk severity and cyberdefence must be concentrated on the most likely severe consequences.
3. Normalization for cyberdefence systems like "computers" is in its infancy, such as standard.
4. Users of the "non-computers" group are very numerous but scattered (vehicles, machines, buildings, etc.). Protecting these systems against cyberattacks is very difficult as it has not been regulated or standardised yet.

Frequency of cyberattack	Consequence of cyberattack			
Frequent	Catastrophic	Critical	Marginal	Negligible
Probable	I	I	I	II
Occasional	I	I	II	III
Remote	I	II	III	III
Improbable	II	III	III	IV
Incredible	III	III	IV	IV
Incredible	IV	IV	IV	IV
I - acceptable risk level ; II - tolerable risk level ; III - tolerable-unacceptable risk level ; IV - unacceptable risk level				

Figure 3. A sample of a cyber risk matrix. ■

Printer security breach? Not on your watch.

Defend your network with the world's most secure printers.

New enterprise HP LaserJets with JetIntelligence provide the industry's deepest printer security.[1] Features including HP Sure Start with its self-healing BIOS, whitelisting, and runtime intrusion detection come built in.
hp.com/go/printersthatprotect

[1] The world's most secure printers and deepest level of security. Based on HP review of 2015 published embedded security features of competitive in-class printers. Only HP offers a combination of security features for integrity checking down to the BIOS with self-healing capabilities. A FutureSmart service pack update may be required to activate security features on the HP LaserJet M527, M506, M577. Some features will be made available as a HP FutureSmart service pack update on select existing enterprise printer models. For list of compatible products visit: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA6-1178ENW. For more information visit: hp.com/go/LJsecurityclaims.
[2] Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study," March 2015.

INTERVIEW WITH JANUSZ KOWALSKI

JANUSZ KOWALSKI
is the Vice-President of the Management Board of PGNiG SA, responsible for Corporate Affairs. He was Deputy Mayor of Opole in 2014-2015. He holds master's degrees in law and administration. In 2006-2007, Mr. Kowalski was an Energy Security Analyst at the Government Proxy Team for Diversification of Energy Supply Sources at the Ministry of Economy. Mr. Kowalski also served as member on supervisory boards of Operator Logistyczny Paliw Płynnych, Investgas SA (PGNiG Group), Ostrołęckie Towarzystwo Budownictwa Społecznego Sp. z o.o. and Energetyka Cieplna Opolszczyzny SA of Opole.

There is a broad discussion about how the NIS Directive (European Directive on the Security of Network and Information Systems) may improve the general level of cybersecurity in the countries of the European Union. From the perspective of PGNiG SA, one of the key actors of the Polish energy sector, which elements of the Directive are the most important and how should Poland go about implementing them?

From our perspective, the most important issues are those concerning access to information on cyberattack threats as well as the sharing of related experience and data. What I mean by this is both the flow of information within the European Union and between the EU member states as well as the transfer of know-how between different entities in Poland itself. It is also extremely important that a single competence centre is established. The centre could be responsible for issuing warnings about cyberthreats, but also act as a kind of repository of data on current and past threats reported by strategic companies operating in the energy sector, or by various public institutions.

The process of implementing the NIS Directive in Poland is coordinated by the Polish Ministry of Digital Affairs. We observe with satisfaction its successive steps, including the establishment of the National Cybersecurity Centre as well as its ongoing efforts to develop the national cybersecurity strategy. Action taken by the Polish authorities is fully consistent with our expectations, as it will allow us to further enhance our own competences and procedures related to ICT security across the PGNiG Group.

Cybersecurity is not an end in itself. Secure ICT systems should allow organisations to run their business processes without any disruption. How should security-related activities be carried out in order to keep up with business and support its operations?

The key is to prioritise appropriately and match bespoke solutions to existing, smoothly running corporate mechanisms. Certainly, the first step should be to set up a team of experts who would not only design and implement standards and develop recommendations concerning the security of ICT systems and networks, but who would also continuously analyse any emerging security threats. To ensure that corporate mechanisms remain highly efficient and that business continues to perform successfully, it is advisable that experts who form such a team understand how organisational units supporting day-to-day business operations work or even that some of them are actually recruited from such units. It seems that such knowledge would guarantee that any security solutions developed by the team do not materially interfere with the technological, financial, or organisational processes of business organisations. This is the philosophy we follow at PGNiG where as early as the stage of designing or modernising processes starts we arrange for a dialogue to enable a mutual understanding of business and security needs. To date, this systemic approach to combining the two areas has worked without fail.

As part of the action scheme dedicated to the cybersecurity of the US critical infrastructure, the National Institute of Standards and Technology (US) published a document entitled "Cybersecurity Framework" that contains standards and guidelines to help improve the security of ICT systems. What is your opinion on this kind of initiatives? Do they really contribute to enhancing the level of cybersecurity?

From the point of view of pursuing enhancements to the security of ICT systems, any such initiatives are certainly very useful. We must remember, though, that the full implementation of such guidelines is not always necessary or even possible. We must keep in mind the various characteristics of legal and organisational environments in different countries as well as the nature of business and technological processes of specific industrial sectors or entities.

What we find highly important and desirable is the measures taken by the Polish institutions responsible for ICT security. For instance, some time ago we were invited to participate in a project aimed at developing a set of standards and good practice to enhance the security of industrial automation systems, launched and coordinated by the Government Centre for Security. This valuable initiative gave us both an opportunity to exchange experience with our peers in Poland, and improve our standards in the area of the security of these specific ICT systems.

During the last year's European Cybersecurity Forum, business representatives pointed out that public-private cooperation, which is essential to ensure cybersecurity, should be based on the mutual engagement of the public and the private sector. What kind of support would you expect from the public sector in the process of ensuring cybersecurity?

I have already mentioned our key needs in the area of improving ICT security. Let me repeat again that the activities and initiatives taken in this respect by the Polish government agencies are going in the right direction. The support we receive from them as the PGNiG Group is adequate. Thinking about developing systemic solutions with respect to ICT security, I agree with the opinion included in your question that the cooperation between the public and business sectors should generally be strengthened and intensified.

Under the NIS Directive you touched upon earlier, all the EU member states are required to compile their lists of entities operating in sectors of strategic importance to the nation and the country's economy. This requirement will narrow down the number of entities subject to the security regime imposed by the Directive; yet it will still be necessary to develop appropriate cooperation mechanisms for each sector. The point is to ensure that, first of all, effective procedures are in place to allow for mutual notification of risks; second, adequate mechanisms exist to share experience in security incident response; and finally, there are powerful strategies for handling crisis situations caused by such incidents. These pose quite a challenge, but we can already say that the PGNiG Group is ready to actively support and participate in any such initiatives. ■

Questions prepared by:
Dr Joanna Świątkowska


NATO Road to Cybersecurity
Wiesław Goździewicz, Mateusz Krupczyński,
Joanna Kulesza, Miron Lakomy, Michał Matyasik,
Kate Miller, Tomasz Romanowski, Ryszard Szpyra,
Magdalena Szwiec, Joanna Świątkowska
Editor: Joanna Świątkowska
The Kosciuszko

ANALYSIS

PROTECTING THE PUBLIC CORE OF THE INTERNET: A DIPLOMATIC AGENDA[1]

DENNIS BROEDERS
Dennis Broeders is professor of Technology and Society at the department of Public Administration and Sociology of the Erasmus University Rotterdam and a senior research fellow at the Netherlands Scientific Council for Government Policy (WRR), an advisory body to the Dutch government within the Prime Minister's department. His research broadly focuses on the interaction between technology and policy, with specific areas of interest in cybersecurity governance, internet governance and Big Data. He recently published the books "The public core of the internet: towards a new international agenda for internet governance" (2015, Amsterdam University Press) and "Exploring the boundaries of Big Data" (2016, Amsterdam University Press).

1. Internet Governance: Between the Technical and the Political

Everyday life without the Internet has become unimaginable. It is rooted in our social lives, our purchasing behaviour, our work, our relationship with the government and, increasingly, in our everyday objects, from smart meters to the cars we drive and the moveable bridges that we cross en route. The Internet is an invaluable source of economic growth and expands the social and cultural horizons of its users. Its openness is the motor behind many industries as well as an industry in itself, providing opportunities for new interfaces between consumers and producers, citizens and governments, and between people on a local, national, and global scale. While it is hard to predict what direction the Internet will take in the coming years and decades, it is safe to say that interconnectedness and interdependence between the online and offline worlds are likely to remain at the core. This makes the functioning and integrity of the Internet as an infrastructure a vital necessity for the future. In turn, this underlines the importance of responsible governance to maintain the functionality and integrity of the internet.

For a long time, Internet governance was the exclusive domain of what is known in Internet circles as the "technical community[2]". That community laid the foundations for the social and economic interconnectedness of our physical and digital lives. Those foundations, with the TCP/IP Protocol Suite as the most prominent component, continue to function as the robust substructure of our digital existence. But the governance of that substructure has become controversial. The many economic and political interests, opportunities, and vulnerabilities associated with the Internet have led governments to take much more interest in the governance of the Internet. Moreover, in terms of policymaking, the centre of gravity has shifted from what was primarily an economic approach (the Internet economy, telecommunications and networks) to one that focuses more on national and other forms of security: the Internet of cybercrime, vulnerable critical infrastructures, digital espionage, and cyberattacks. In addition, a growing number of countries seek to regulate their citizens' online behaviour, their reasons ranging from copyright protection and fighting cybercrime to censorship,

1 | This paper is based on the Dutch report De publieke kern van het internet that the Netherlands Scientific Council for Government policy presented to Bert Koenders, Dutch minister of Foreign Affairs, on 31 March of 2015. The English version was published as: Broeders D., report "*De publieke kern van het internet*" that the Amsterdam University Press 2015. Available at: http://www.wrr.nl/fileadmin/en/publicaties/PDF-Rapporten/The_public_core_of_the_internet_Web.pdf.

2 | This community includes – but is not limited to – organisations such as the Internet Architecture Board (IAB), the Internet Engineering Taskforce (IETF), and the World Wide Web Consortium (W3C) that develop protocols and standards and organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registries (RIRs) that deal with the distribution of Internet resources such as IP numbers and domain names. Also, the global informal community of CERTs or CSIRTs can be considered part of the technical community.

surveillance, and control of their own populations on and through the Internet.

Increasingly, governments view the core infrastructure and main protocols of the Internet itself as a legitimate means to achieve their policy ends. Whereas Internet governance used to mean governance of the Internet, today it also means governance using the architecture of the Internet[3]. In that second notion, the Internet becomes a policy instrument to achieve other (national) policy goals. Such interventions may have huge implications for core Internet infrastructures and protocols and, in turn, for the digital lives that we have built on top of them. Such interventions can undermine the integrity and functionality of the Internet. If the Internet ceases to operate, many processes and routines, from the trivial – our Facebook status – to the essential – payment transactions – will grind to a halt. If the core protocols of the Internet are corrupted, the Internet becomes unreliable. Who would risk online banking in that case? If we cannot be sure that data will be sent and arrive at its intended destination, that will influence the kinds of economic and social processes that we do or do not entrust to the Internet. Would we let the Internet handle our private and work-related communications in that case? If we know that security gaps are deliberately being built into Internet standards, protocols, hardware and software to guarantee foreign intelligence and security services access, then our confidence in the Internet will gradually crumble. If more and more countries withdraw behind digital borders, the Internet will no longer operate as an international infrastructure as it has done so far. And in the worst-case scenario, the exploitation of vulnerabilities in core Internet protocols and infrastructures could lead to serious breakdowns in society and economy.

This paper, therefore, argues that the core of the Internet must be regarded as a global public good. As such, it should be protected against the interventions of states that are acting in their own national interest, and intentionally or unintentionally damage that global public good, which may erode public confidence in the Internet. In that respect, Internet governance is at a crossroads: the Internet has become so important that states are no longer willing or able to regard it with the same "benign neglect" that long set the tone for most countries. At the same time, however, states do have national interests that go beyond the governance of the Internet as a collective infrastructure. For the future of Internet governance, it is imperative to determine what part of the Internet should be regarded as a global public good – and thus safeguarded from unwarranted interference by states – and what part should be seen as the legitimate domain of national states[4], where they can claim a position and take up their role without harming the logical and technical infrastructure of the Internet itself.

2. Towards a New International Agenda For Internet Governance

Growing state interference with core infrastructure and protocols of the Internet underlines the need for a new international agenda for Internet governance that begins with the notion of a global public good.

2.1 A Global Public Goods Approach of Internet Governance

Some core protocols and infrastructure of the Internet can be considered a global public

3 | For an elaboration on this distinction, see DeNardis L., *Hidden levers of internet control. An infrastructure-based theory of internet governance*, "Information, Communication and Society" 2012, 15 (5), p.726; DeNardis L., *Internet points of control as global governance*, CIGI Internet Governance Papers nr. 2, August 2013; and DeNardis L., *The global war for internet governance*, Yale University Press 2014.

4 | This paper focuses on the behaviour of states. Obviously the behaviour of companies, or other non-state actors, may also have negative implications for the public core of the Internet, but they are not explicitly dealt with here.

good. Global public goods produce benefits to everyone in the world; benefits that can be gained or preserved only by taking specific action and by cooperating. The means and methods for providing a global public good may differ from one case to another; they can also be undertaken by private or public parties, or combinations of the two[5].

> “As a public good, the Internet only works properly if its underlying values – universality, interoperability, and accessibility – are guaranteed.

This can be said to apply to the Internet as a network and as an infrastructure. If key protocols like TCP/IP, DNS and routing protocols do not work properly, the Internet's very operation will come under pressure. If these protocols are corrupted, everyone loses. The Internet is “broken” if we can no longer assume that the data that we send will arrive, that we can locate the sites we are searching for, and that those sites will be accessible. As a public good, the Internet only works properly if its underlying values – universality, interoperability, and accessibility[6] – are guaranteed and if it facilitates the main objectives of data security, i.e. confidentiality, integrity, and availability[7]. To phrase it in a more functional terminology: anything that hampers or interferes with the global availability and integrity of the core forwarding and naming functions of the Internet, can be perceived as negative to the public core of the Internet[8]. It is vital that we – the users – can rely on the most fundamental Internet protocols functioning properly. After all, these protocols underpin the digital fabric of our social and economic life. Our confidence in the integrity and continuity of all we have built on the public core of the Internet – our digital existence – very much depends on those underlying protocols.

The importance of properly functioning Internet protocols and infrastructure seems obvious because it is these protocols that guarantee the reliability of the global Internet. Yet, recent international trends in policymaking and legislation governing the protection of copyright, defence and national security, intelligence and espionage, and various forms of censorship show signs of actual and possible interventions that may damage the core. Some states see DNS, routing protocols, Internet standards, the manipulation and building of backdoors into software and hardware, and the stockpiling of vulnerabilities in software, hardware and protocols (so called “zero days”) as legitimate instruments for national policies intent on monitoring, influencing, and blocking the conduct of people, groups, and companies. Some of these may have a global impact. However, the negative impact of such interventions in the public core of the Internet falls to the collective, and impairs the Internet's core values and operation. Illustrations of this trend include[9]:

5 | Lieshout P. Van, R. Went and M. Kremer, *Less Pretension, More Ambition development policy in times of globalization*, Amsterdam University Press 2010, pp.190-192, see op. cit. Broeders D., 2015, pp.19-20 for the application to core Internet protocols and infrastructure. As it is technically possible to exclude people from the Internet, economists usually refer to it as a “club good”, i.e. a good whose benefits accrue only to members. Our reference to the Internet's core as an impure global public good is based on the technical and protocol-related set-up of the Internet with universality, interoperability and accessibility as its core values, which underscore the values of non-rivalry and non-excludability.

6 | See for example op. cit. DeNardis, 2013, p.4.

7 | See for example Singer P. and A. Friedman, *Cyber security and cyber-war. What everyone needs to know*, Oxford University Press 2014, p.35.

8 | As it was phrased in an international workshop on the Public core of the Internet organised by the Dutch Ministry of Foreign Affairs in The Hague on 11 July 2016.

9 | For a fuller discussion of these trends see op. cit. Broeders, 2015, especially chapters 3 and 4.

- Various forms of Internet censorship and surveillance[10] that use key Internet protocols and may result in over blocking[11], as well as enlisting the "services" of Internet intermediaries such as Internet Service Providers (ISPs) to block and trace content and users[12].

– The transition of the "IANA function", which includes the stewardship and maintenance of registries of unique Internet names and numbers. There is currently a transition underway which will remove oversight of IANA from the US's sphere of influence, mainly for reasons of international political legitimacy[13]. The debate on this transition may result in more politicised management of the Domain Name System, which, in turn, may have repercussions for the ability to find and locate sites and users. Most countries would benefit from IANA functions that are as "agnostic" as possible, especially when it comes to the administrative tasks[14].

– The online activities of military cyber commands, intelligence and security services, and sometimes even law enforcement agencies which undermine the proper functioning of the public core of the Internet. By corrupting Internet standards and protocols[15], by building backdoors into commercial hardware and software[16], and by stockpiling zero-day vulnerabilities[17], these actors effectively damage the collective Internet infrastructure and make it less secure. Moreover, they create a digital version of the "security dilemma", in which the use of cyberspace as an instrument for national security, in the sense of both cyberwarfare and mass surveillance by intelligence services, undermines the overall level of cybersecurity on a global scale[18].

– Legislation to protect copyright and intellectual property that permits the use of vital Internet protocols to regulate and block content. The "side-effects" of such legislation include the collateral blocking of content and users ("over blocking"), damage to DNS, and intermediary censorship through ISPs[19].

10 | For the development of state censorship see: Deibert R., *Black code. Inside the battle for cyber space*, Signal 2013; Deibert, R., et al. (red.), *Access denied: The practice and policy of global internet filtering*, MIT Press 2008; Deibert, R., et al. (red.), *Access controlled: The shaping of power, rights, and rule in cyberspace*, MIT Press 2010; Deibert, R., et al. (red.), *Access contested. Security, identity, and resistance in Asian cyberspace*, MIT Press 2011; and op. cit. DeNardis, 2014, chap. 9.

11 | For example, when Pakistan wanted to block YouTube because it violated its blasphemy laws, the implementation by Pakistan Telecom was technically inadequate, so it ended up blocking YouTube on large parts of the Internet, see op. cit. DeNardis, 2014, p.96.

12 | See for example Zuckerman and MacKinnon who warn of intermediary censorship and the outsourcing of censorship respectively: Zuckerman E., *Intermediary censorship*, in op. cit. Deibert et al, 2010, pp.71-85; MacKinnon R., *Corporate accountability in networked Asia*, in op. cit. Deibert et al., 2011, p. 197.

13 | See for example Taylor E., *ICANN: Bridging the Trust Gap*, Ourinternet.org, Paper series, nr. 9, CIGI 2015. For more information on the so-called IANA transition see: https://www.icann.org/stewardship-accountability.

14 | See Mueller M. and B. Kuerbis, *Towards global internet governance: How to end U.S. control of ICANN without sacrificing stability, freedom or accountability*, TPRC Conference Paper 2014, available at: http://ssrn.com/abstract=2408226.

15 | For example, it seems from the Snowden files that the NSA worked to weaken and corrupt encryption standards that are meant to secure Internet traffic, see Landau S., *Making Sense of Snowden Part II: What's Significant in the NSA Surveillance Revelations*, "IEEE Security and Privacy", Vol. 12, No. 1, Jan./Feb. 2014.

16 | See for example Greenwald G., *No place to hide. Edward Snowden, the NSA and the US Surveillance State*, Metropolitan Books 2014; and Hoboken J. van and I. Rubinstein, *Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the post-Snowden era*, "Maine Law Review", 2014, 66 (2), pp.487-534.

17 | See for analyses of the zero day markets: Stockton P. and M. Golabek-Goldman, *Curbing the market for cyber weapons*, "Yale Law and Policy Review", 2013, 32 (1), pp. 101-128; and Fidler M., *Anarchy or regulation? Controlling the global trade in zero-day vulnerabilities*, Honors thesis in International Security Studies, Stanford University, 2014.

18 | Dunn Cavelty M., *Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities*, "Science and Engineering Ethics", 2014, 20 (3), pp. 701-715.

19 | In general, see for example: Zittrain J. and Palfrey, *Internet filtering: The politics and mechanisms of control*, in op. cit. Deibert, 2008, pp. 29-56; Mueller M., *Networks and states. The global politics of internet governance*, MIT Press 2010, chap. 7; Yu P.K., *Digital copyright enforcement measures and their human rights threats*, in C. Geiger (ed.), *Research Handbook on Human Rights and Intellectual Property*, Edward Elgar 2014; for the influence on key protocols see op. cit. Broeders, 2015, pp.71-72.

– Some forms of Internet nationalism and data nationalism – in which states seek to fence off a national or regional part of the Internet – that require interventions in routing protocols. In extreme forms this may splinter the Internet[20].

A number of powerful states have built up significant cyber capacity in the military and intelligence domain and are well ahead of the rest in this trend.

But many countries are now in the midst of digitising their state, economy and society as well as building civic and military cyber capacity[22]. Moreover, the Internet is undergoing a demographic shift in which the centre of gravity is moving from the North and West to the East and South of the planet[23]. Figure 1 shows worldwide Internet penetration and the regions where there is the most room for growth. The lighter the colour, the more potential there is for an increase in the number of Internet users.

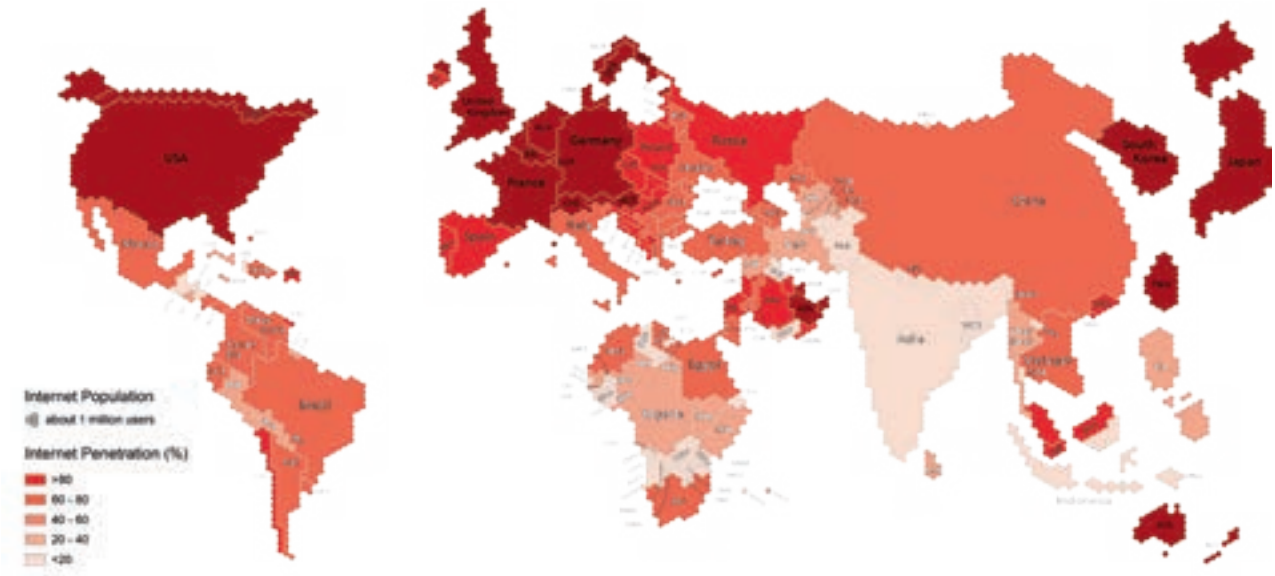


Figure 1. Internet users and internet penetration worldwide, 2011[21].

This shift has major consequences for the balance of power on the Internet and for how states view cyberspace culturally and politically. When the next billion (or billions) of users go online in the years ahead, these emerging states will develop their own national policies in relation to the online world and will have to ask themselves whether or not they will use the public core of the Internet

20 | See Maurer et al, *Technological sovereignty: Missing the point? An analysis of European proposals after June 5, 2013*, Report for Transatlantic Dialogues on security and freedom in the digital age, 2014; Chander A. and U. Le, *Breaking the Web: Data localization vs. the global internet*, "Emory Law Journal" 2014, although they see problems with almost all forms of data nationalism, not just those that require blocks in routing protocols. See also Drake W., V. Cerf and W. Kleinwächter, *Internet Fragmentation: an overview*, "Future of the Internet Initiative White Paper", January 2016, World Economic Forum, pp. 41-48.

21 | Source: Graham M., De Sabbata S., and Zook M., *Towards a study of information geographies: (im)mutable augmentations and a mapping of the geographies of information*, "Geo: Geography and Environment", 2015, Vol. 2 (1), p.92.

22 | See Lewis J., *Cybersecurity and cyberwarfare: assessment of national doctrine and organization*, in UNIDIR, *The Cyber Index. International Security Trends and Realities*, United Nations Institute for Disarmament Research, 2013, for some indications of the build-up of civic and military cyber capacity globally.

23 | Op. cit. Deibert, 2013, chap.5; see also Choucri N., *Cyberpolitics in international relations*, MIT Press 2012, chap.3.

instrumentally in their efforts. Some of these countries have authoritarian regimes with a history of controlling and sometimes repressing their own population, and using modern technology to do so. There is no guarantee that these countries will spare the Internet's public core as their societies continue to digitise. In addition, many countries will have considerably upgraded their technical cyber capacity in a few years, giving a much larger group of states the capacities that are currently reserved for only a few superpowers. What is cutting-edge now will be common in five years' time. If in that same time the idea takes hold that national states are at liberty to decide whether or not to intervene in the Internet's main protocols and infrastructure to secure their own interests, the impact on the Internet as a public good may be very damaging.

2.2 Making The Public Core of The Internet an International Neutral Zone

Given these developments, it should be an internationally shared diplomatic priority to work towards establishing an international norm that identifies the main protocols of the Internet as a neutral zone in which governments are prohibited from interfering for the sake of their national interests. This should be considered an extended national interest[24], i.e. a specific area where national interests and global issues coincide for all states that have a vital interest in keeping the Internet infrastructure operational and trustworthy. With the continuing spread of the Internet and ongoing digitisation, that is increasingly a universal concern.

In order to protect the Internet as a global public good, there is a need to establish and disseminate an international norm stipulating that the Internet's public core – its main protocols and infrastructure, which are a global public good – must be safeguarded against unwarranted intervention

> "It should be a diplomatic priority to work towards establishing an international norm that identifies the main protocols of the Internet as a neutral zone.

by governments. The starting point should be to place the drafting of such a standard on the international political agenda, something that will require making governments around the world aware of the collective and national importance of this neutral zone. Given the enormous differences between countries in terms of Internet access, overall digitisation and technological capacity, this will require a serious diplomatic and political effort. This standard could be disseminated through relevant UN forums as well as through regional organisations such as the EU, the Council of Europe, the OECD, the OSCE, ASEAN and the AU. This strategy would lay the foundations for what could eventually expand into a broader regime.

Given the rising conflict between national security and Internet security, there is a need to separate and disentangle the various forms of security relating to the Internet. The increased emphasis on national security has had a negative impact on the debate on cybersecurity. Some researchers maintain that cybersecurity and cyberwarfare have become part of a "securitised" discourse[25]. Many governments are seriously investing in capacity building in the realm of national and international cybersecurity in response to what is a relatively poorly defined threat. The term "threat inflation" is often used to explain the rapidly expanding cybersecurity budgets and legislated powers,

24 | Knapen B. et al., *Attached to the World. On the anchoring and strategy of Dutch foreign policy*, Amsterdam University Press, 2011, pp. 45-48.

25 | Hansen L. and H. Nissenbaum, *Digital disaster, cyber security and the Copenhagen School*, "International Studies Quarterly" 2009, 53, pp. 1155-1175; Dunn Cavelty M., *From Cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse*, "International Studies Review" 2013, 15 (1), pp. 105-122; op. cit. Singer and Friedman, 2013.

especially in the United States[26]. This could lead to a far-reaching militarisation of the cyber domain[27], the rise of a new cyber military-industrial complex[28], and even an arms race in cyberspace[29]. This is in spite of the fact that initial attempts to study how the law of armed conflict applies to cyber conflicts, such as the Tallinn Manual on the International Law Applicable to Cyber Warfare[30], show that, so far, not a single cyber incident conforms to the legal definitions of "war"[31].

2.3 Disentangling Internet Security and National Security

The emerging emphasis on national security comes at the expense of a broader range of views on security and the Internet. Defining and disentangling various views on security may in fact improve the security of the Internet as an infrastructure. It is, therefore, vital to advocate internationally for a clear differentiation between Internet security (security of the Internet infrastructure) and national security (security through the Internet) and to disentangle the parties responsible for each. It is of paramount importance to delineate the various forms of security in relation to the Internet. On one end of the spectrum there is the notion of Internet security, i.e. ensuring that the network itself is secure and operational. On the other end, there is the notion of national security, with the focus on the state and the Internet being regarded simultaneously as a source of threat and as a potential policy tool. Between the two ends of the spectrum is a view that focuses more on cybercrime and has law enforcement as the primary national, regional, and international actors.

Internet security denotes the security of the Internet as a global infrastructure and has traditionally been the concern of the technical community. It is a network and technology-driven strategy, such as that of the Computer Emergency Response Teams (CERTs) which involves a public health-type approach to overall network security. The aim is to maintain the health of the Internet as a network for the benefit of all users[32]. Trust and a shared understanding of the Internet and network security as well as information-sharing have been key ingredients contributing to the gradual growth of international cooperation between various CERTs. It is important not to confuse and/or mix this logic with that of national security, which places national interests above network interests. Importantly, a strict division is required between the actors responsible for national security, such as the military and the intelligence and security services, and parties such as CERTs that safeguard the security of the Internet itself. Confusing the two logics, or letting national security logic dominate, could seriously impair the mutual trust that the technical community has managed to build over the course of many years. These two forms of security, and the actors responsible for them, should remain separate, even in periods when the security of the online and offline world is under threat. Indications of movement on this

26 | Libicki M., *Cyberspace is not a warfighting domain*, "I/S: A Journal of Law and Policy for the Information Society" 2012, 8 (2), pp. 321-336; Lin H., *Thoughts on threat assessment in cyberspace*, "I/S: A Journal of Law and Policy for the Information Society" 2012, 8 (2), pp. 337-355; Rid T., *Cyber war will not take place*, Hurst and Company 2013.

27 | Op. cit. Libicki, 2012; Dunn Cavelty M., *The militarisation of cyberspace: Why less may be better*, pp. 141-153, in C. Czossceck, et al. (red.), *4th International Conference on Cyber Conflict*, NATO CCDCOE Publications 2012.

28 | Brito J. and T. Watkins, *Loving the cyber bomb? The dangers of threat inflation in cyber security policy*, "Harvard National Security Journal" 2011, 3 (1), pp. 41-84; op. cit. Deibert, 2013.

29 | Nye J. Jr., *Nuclear lessons for cyber security?*, "Strategic Studies Quarterly" 2011, 5 (4), pp. 8-38.

30 | Schmitt M. (ed.), *Tallinn Manual on the international law applicable to Cyber Warfare*, Cambridge University Press 2013; the Tallinn Manual 2.0 is also nearing completion. The focus of the original Tallinn Manual is on the most disruptive and destructive cyber operations – those that qualify as "armed attacks". The Tallinn 2.0 project examines the international legal framework that applies to malevolent cyber operations that do not rise to the aforementioned levels, yet are a daily challenge to states. See: https://ccdcoe.org/research.html.

31 | AIV/CAVV, *Cyber Warfare*, nr. 77, AIV/ nr. 22, CAVV, Advisory Council on International Affairs, 2011; see also op. cit. Rid, 2013.

32 | See for example JPCERT/CC, *The cyber green initiative: Improving health through measurement and mitigation*, JPCERT/CC Concept Paper, 10 August 2014.

issue can be found in the latest report of the UN GGE, for example in its argument that states are urged to "neither harm the systems and activities of other (national) CERTs, nor to use their own to engage in malicious international activity"[33]. Nor should these types of actors be mixed under the pressure of budgetary restraints and a scarcity of qualified computer experts that is felt by various government agencies active in the broader field of cybersecurity[34].

The process of debating the highest levels of national security – military cyber commands and intelligence and security services – is both the most crucial and the most complicated from the perspective of restraining government behaviour. Considerations of state sovereignty make regulating these actors through international law or agreements a highly complex affair. There are, of course, various initiatives underway to arrive at international norms, but these are mainly set within the context of international security and are intended to prevent escalation between states. The Groups of Governmental Experts (GGEs) and other initiatives of this kind emphasize codes of conduct and the Confidence-Building Measures that are meant to prevent states from misinterpreting each other's conduct online[35]. A clear division between different forms of security and the demarcation of the domains of the various actors involved could help these ongoing international deliberations about standards in cyberspace. In fact, a more precise terminology and a clear division of labour between various agencies can, in itself, function as a confidence building measure in the international cyber domain.

3. Broadening The Diplomatic Arena

The demographic shift on the internet and the rise of new big and mid-level powers in internet affairs challenges the still very dominant transatlantic take on internet governance. A recent report by the Council on Foreign Relations called on the US government to make this new reality the basis for its foreign cyber policy: "The United States can no longer rely on its role as the progenitor of the internet to claim the mantle of leadership"[36]. Snowden's revelations have caused that mantle to slip further by undercutting the US's moral leadership in Internet matters. By extension, the "Western" voice is seeing its dominance in the debates about Internet governance challenged. It is, therefore, time to open, broaden,

"The demographic shift on the internet and the rise of new big and mid-level powers in internet affairs challenges the still very dominant transatlantic take on internet governance.

and expand the arena for cyber diplomacy. There is a need to involve states that are still building their technical and political cyber capacities – for example the so-called "swing states"[37] – integrally in debates about Internet governance and cybersecurity. Secondly, there is a strong case to be made for targeting the big Internet-based companies as explicit subjects of cyber diplomacy.

33 | See paragraph 13(k) of the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security 2014-2015, Report as adopted, Friday 26 June. Available at: http://undocs.org/A/70/174.

34 | Broeders D., *Investigating the place and role of the armed forces in Dutch cyber security governance*, The Netherlands Defence Academy, 2014, pp. 38-40.

35 | Kane A., *The rocky road to consensus: The work of UN groups of governmental experts in the field of ICTs and in the context of international security*, 1998-2013, "American Foreign Policy Interests" 2014, 36 (5), pp. 314-321; Hurwitz R., *The play of states: Norms and security in cyberspace*, "American Foreign Policy Interests" 2014, 36 (5), pp. 322-331.

36 | Council on Foreign Relations, *Defending an open, global, secure and resilient internet*, Council on Foreign Relations, 2013, p.67.

37 | Maurer T. and R. Morgus, *Tipping the scale: An analysis of global swing states in the internet governance debate*, CIGI Internet Governance papers no. 7, May 2014.

3.1 Building New International Coalitions

The challenge for Internet governance is how to build new, broad coalitions that are willing to support a norm that protects the public core of the Internet. While the "usual suspects" in the transatlantic axis, i.e. the EU and the OECD, are still important actors in Internet governance, the bigger challenge lies elsewhere. The conversation between "like-minded" allies will help to bring the desired standards and norms into focus, but the real impact in this arena will come from a dialogue with states that are outside that circle[38].

That became clear during the 2012 World Conference on International Telecommunications in Dubai, when it came time to vote on the International Telecommunications Regulations (ITRs). The Western camp found itself in the minority when its members voted against new ITRs that would increase the state influence over the Internet and could open the door to some degree of nationalisation. Some 89 states, including China, Russia and many Arab nations, voted in favour, while 55 others, including the member states of the EU, the US, and most members of the OECD, voted against. In Figure 2 – based on ITU data – the opposing countries are coloured red and those in favour of the new ITRs are coloured black. The votes of the countries in grey were not formally registered due to outstanding membership fees. In diplomatic terms, it is clear that there is much to be gained by engaging with the large group of countries that have not yet taken up a firm position on various issues of Internet governance and cybersecurity.

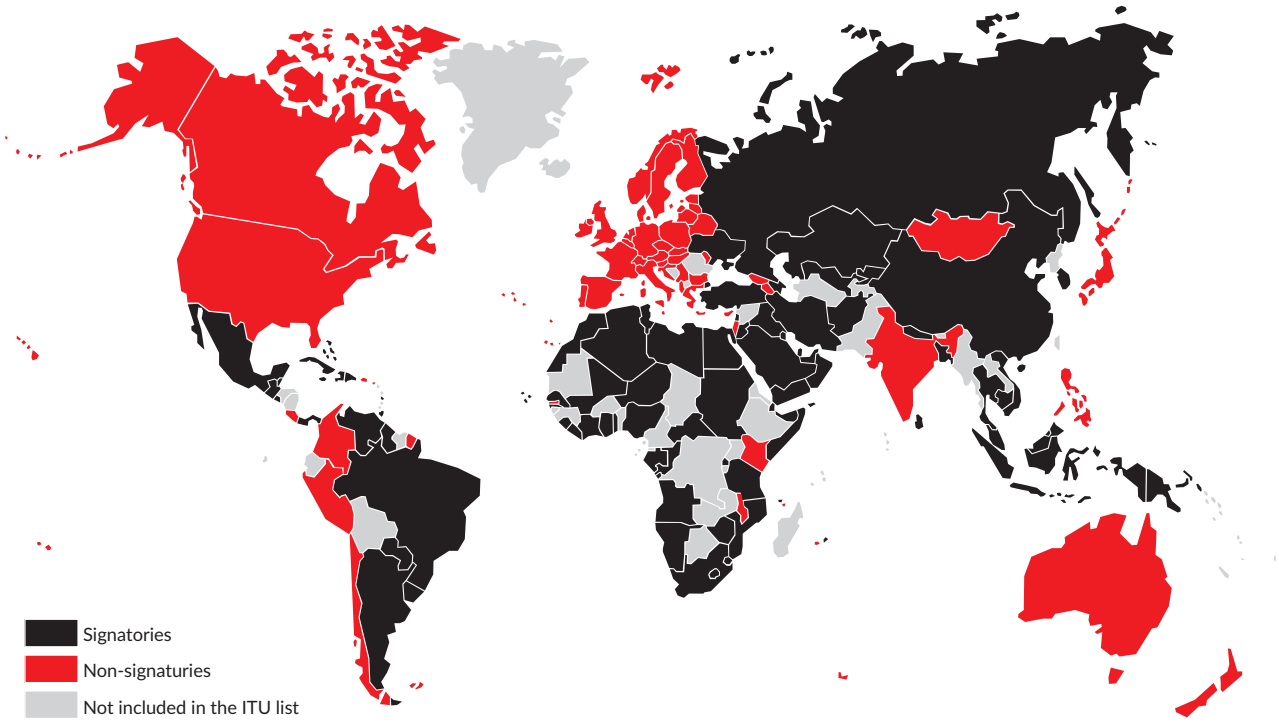


Figure 2. Voting results on the ITRs, WCIT, Dubai 2012[39].

38 | Op. cit. Hurwitz, 2014, p.330.

39 | Source: Techdirt.com, http://tnijurl.com/ituvote.

> There is much to be gained by engaging with the large group of countries that have not yet taken up a firm position on various issues of Internet governance and cybersecurity.

Many states are still developing their strategy, policy and capacity to engage with Internet governance issues, especially at the international level. Diplomatic efforts focused on securing the public core of the Internet will only succeed through effective engagement with these states, which could represent a political middle ground between the two extremes in the discussion. Maurer and Morgus[40] identified a top thirty swing states worldwide by combining the voting results for the new international telecommunications treaty with a broad range of criteria, including membership of international organisations and degree of democratisation. They also looked at Internet penetration, the presence of an active Internet community, and the size of the digital economy.

These swing states are neither the "like-minded" states of the "Western camp" nor the "other-minded" states with repressive and dictatorial regimes. Nor are they very small states or states with few resources that are considered to have little influence. As such, they are an important starting point for building new coalitions and broadening existing ones. It should also be noted that the digital superpowers of today – at least in terms of numbers of Internet users – will not necessarily be the superpowers of tomorrow. The southward and eastward demographic shift that is unfolding in cyberspace underlines the importance of involving the swing states in the diplomatic effort to establish the norm that it is in the interest of all countries not to interfere with the Internet's public core.

40 | Op. cit. Maurer and Morgus, 2014.

3.2 Including Private Companies in the Diplomatic Dialogue

In the predominantly privately owned and run world of the Internet, Apple, Google, Huawei, Microsoft and other corporate giants are forces to be reckoned with. It is they who largely decide what our online lives look like and what new directions the information society will take. This also means that, more than in the past, these corporations should be approached from the perspective of diplomacy and the rule of law. This is a matter of power and counter-power, and – as in diplomatic relationships between states – the interests and agendas of such corporations will sometimes align and sometimes conflict with national and collective interests[41]. For example, it is not clear why most Western countries maintain a dialogue about human rights with authoritarian regimes, but not with companies that are vital to the protection of privacy and freedom of communication around the world[42]. Given that large Internet companies are powerful and influential actors in Internet governance, they should be much more explicitly part of the diplomatic arena. Relevant issues include privacy and data protection, market dominance, the security of hardware and software, and data protection by means of encryption. Many governments are relatively weak parties in their dealings with these private-sector giants, for reasons of size and resources, and also because of economic interests and dependencies in relation to these corporations. Regional organisations such as the EU sometimes take a stand. But even though the EU's political force is considerable, its gears grind slowly compared to the fast-paced Internet economy. That much became clear in the infamous case that the European Commission brought against Microsoft under EU competition law. While

41 | Broeders D. and L. Taylor, *Does great power come with great responsibility? The need to talk about Corporate Political Responsibility*, in: L. Floridi and M. Taddeo (eds.), *Understanding the responsibilities of Online Service Providers in information societies*, Springer, 2016.

42 | AIV, *The Internet. A Global Free Space With Limited State Control*, Advisory Council on International Affairs, 2014, p. 63.

the fine was high and proportional (USD 860 million), the proceedings took so long that it was tantamount to "solving the antitrust problem long after the competitors have died"[43]. Nevertheless, the authority to levy heavy sanctions – the recently adopted EU data protection regulation creates the possibility to impose fines between 2% and 4% of annual worldwide turnover – gives the EU and its member states more muscle in their dialogue with these companies. The "shadow of hierarchy" can be an important incentive for private parties to engage in a serious and constructive dialogue with states[44].

Recently, there has been informal resistance from Internet companies against governments, and against the US in particular. Much of it has been driven by Snowden's revelations, which have seriously damaged the reputation of a number of leading American Internet companies among Internet users.

> "Given that large Internet companies are powerful and influential actors in Internet governance, they should be much more explicitly part of the diplomatic arena.

Snowden's files put some big Internet-based companies on the spot as they were – intentionally or unintentionally – the sources of masses of data collected by the intelligence services. These companies are now responding by issuing transparency reports that disclose – as far as the law permits – what data or records governments request or demand, and by tightening up the encryption of their data transports[45]. Although much of this can be explained as an opportunistic drive to retain and/or regain customers, it is an interesting development in terms of power and counter-power.

By raising the cost of mass surveillance through better encryption and maybe even forcing intelligence services to fine-tune their surveillance, their response can be seen as a first move towards counter-power. Microsoft fought a legal battle against the US government's assertion that all data managed by a US company – even if it is held on servers in Ireland – can be commandeered by the government[46]. In July 2016, a US federal appeals court ruled in Microsoft's favour[47]. In light of their market power and the crucial role they play in digitising the lives of entire populations, governments can no longer avoid diplomatic dealings with these information giants. These companies are more than potential investors that must be seduced and recruited; they are more than violators of privacy that must be tackled: they are parties who merit serious diplomatic attention, with all the contradictions inherent to diplomacy.

Steps Towards Protecting the Public Core of the Internet

Ideas similar to the protection of the public core of the Internet have been put on the agenda. In January 2016, William Drake, Vinton Cerf and Wolfgang Kleinwächter, published an excellent paper on the issue of Internet Fragmentation for the World Economic Forum[48]. Some forms of Internet fragmentation – those that may have severe, long-term consequences for the functioning of the Internet as a global infrastructure – are akin to the notion of the public core of the Internet. In June 2016, the Internet Society (ISOC) published a beta version of its Policy Framework for an open and trusted Internet in which it states

43 | Brown I. and C. Marsden, *Regulating code: Good governance and better regulation in the information age*, MIT Press, 2013, p.40.
44 | Börzel T. and T. Risse, *Governance without a state: Can it work?*, "Regulation & Governance" 2010, 4 (2), p.114.
45 | Op. cit. Van Hoboken and Rubinstein, 2014.
46 | See for example: http://www.theguardian.com/technology/2014/dec/14/privacy-is-not-dead-microsoft-lawyer-brad-smith-us-government.
47 | See: https://www.theguardian.com/technology/2016/jul/14/microsoft-emails-court-ruling-us-government.
48 | Op. cit. Drake, Cerf and Kleinwächter, 2016.

that the technical community shares "a sense of collective stewardship towards the public core of the Internet and the open standards on which its technologies and networks are based"[49]. Also in June 2016, the Global Commission on Internet Governance (the Bildt Commission) published its final report called One Internet, which included a policy recommendation on the protection of the public core that read: "Consistent with the recognition that parts of the Internet constitute a global public good, the commission urges member states of the United Nations to agree not to use cyber weapons against core infrastructure of the Internet"[50]. In the Netherlands, the Dutch government issued its formal response to the report on the Public core of the Internet in May 2016, making the protection thereof a long-term priority for its foreign policy on cyber issues[51]. The first opportunity to work on establishing a norm protecting the public core of the Internet will be the 2016-2017 round of the UN GGE, of which the Netherlands is a member. These first steps towards creating awareness and protecting the public core of the Internet will hopefully echo in other diplomatic fora in the years to come. ■

49 | Internet Society, A *policy framework for an open and trusted Internet An approach for reinforcing trust in an open environment*, 2016, p.7.
50 | Global Commission on Internet Governance, *One Internet*, Centre for International Governance Innovation and Chatham House, 2016, p.75. Available at: http://tnijurl.com/ourinternetorg.
51 | See: http://tnijurl.com/dutchreportpubliccore.

TOGETHER WE CAN SEE MORE BUSINESS OBJECTIVES

We have experience, knowledge and skills
that support every business:

- we offer modern cash management
- we base on our rich experience and financial capital
- we structure corporate finances
- we co-finance projects with EU funds
- we enable alternative financing methods (leasing, factoring)

Bank Polski

www.pkobp.pl, helpline: 801 36 36 36, +48 61 855 94 94 cost according to the operator's tariff
Detailed information about the products, and the List of bank fees and charges are available in Regional Corporate Centers of PKO Bank Polski and on the website www.pkobp.pl.

ANALYSIS

WELCOME TO THE ERA OF COGNITIVE SECURITY

MARTIN BORRETT

Martin Borrett is an IBM Distinguished Engineer and CTO IBM Security Europe. He advises at the most senior level in clients on policy, business, technical and architectural issues associated with security. Martin leads IBM's Security Blueprint work and is co-author of the IBM Redbooks "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security" and "Understanding SOA Security". He is Chairman of the European IBM Security Board of Advisors, member of the Royal Society's Cybersecurity Research Steering Group, represents IBM at GFCE, is a Fellow of the British Computer Society, a Chartered Engineer (CEng) and member of the IET.

Today marks the rise of the new cognitive era. Cognitive computing has the ability to tap into and make sense of security data that has previously been dark to an organization's defences, enabling security analysts to gain new insights and respond to threats with greater confidence at scale and speed. Like an analyst, a cognitive system can learn as it goes, able to recognise terms and make connections between them, so it can understand questions and use reason to provide answers.

80% of the World's Data Has Been Invisible, Until Now

The volume of security data presented to analysts is staggering. The average organization sees over 200,000 pieces of security event data per day[1], with enterprises spending $1.3 million a year dealing with false positives alone, wasting nearly 21,000 hours[2]. Couple this with 75,000-plus known software vulnerabilities reported in the National Vulnerability Database, 10,000 security research papers published each year and over 60,000 security blogs published each month[3] – and security analysts are severely challenged to move with informed speed. It takes constant monitoring and maximum use of data to find attacks and abnormal behaviour before the damage is done.

But the world produces over 2.5 quintillion bytes of data every day, and 80% of it is unstructured[4]. This means that it is expressed in a natural language – spoken, written or visual – that a human can easily understand but traditional security systems cannot. The reality is that there are thousands of security blogs posted every day with detailed threat intelligence. But it is impossible for a security analyst to know everything that is in them, and traditional security is unable to analyse and apply this insight the way an analyst can. This is why the most challenging security problems still require people to make sound decisions about what to act on and what to consider a false alarm. In fact, the best security professionals build their body of knowledge every day through experience, talking with colleagues, attending conferences, and keeping up-to-date with research.

Meet Cognitive Security

For almost a century, we have programmed computers to help solve complex problems. We can now simulate weather, sequence genomes, and instantly share data across the world. But ask a computer to do something humans do every day – recognise an image, read a book or explain the meaning of a poem – and it is a different story. Traditional systems fall short. The same is true for security. For decades, we have programmed computers to recognize viruses, malware, and exploits. We continuously tune them to become

1 | IBM Security, 2015 Cybersecurity Intelligence Index, Research Report, 2015

2 | Ponemon Institute, *The Cost of Malware Containment*, Research report, January 2015, available at: http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf.

3 | See IBM X-Force Threat Intelligence Reports, available at: https://securityintelligence.com/media/xforce-tir-2016.

4 | According to Dr John Kelly, Senior Vice President at IBM Research, speech available at https://youtu.be/q7qElhGv7uY.

more accurate, but it is not enough. Adversaries constantly morph their attacks and find creative ways to breach defences. What organizations need is the ability to detect the subtlest change in activity and analyse it with as much context as possible to distinguish and eliminate new threats.

> “ What organizations need is the ability to detect the subtlest change in activity and analyse it with as much context as possible.

At IBM Security, we are training a new generation of systems like the first of a kind *IBM Watson for Cyber Security* to understand, reason, and learn about constantly evolving security threats. We are beginning to build security instincts and expertise into new defences that analyse research reports, web text, threat data, and other security-relevant structured and unstructured data – just like security professionals do every day – but at a scale like we have never seen before. This is the essence of cognitive security. Imagine a typical day for security analysts using cognitive system for cybersecurity. They would come into the office and, with their trusted *Watson* security adviser, could quickly and accurately analyse graphic representations of emerging threats that might impact their organisation. Since *Watson* will have read the latest reports and applied them to events in the organisation's environment, it can respond to natural-language questions. Security professionals will be able to be more proactive, spending less time on the mundane and more on the important work of stopping attacks and protecting their enterprise.

What Is Cognitive Security?

Cognitive systems are self-learning systems that use data mining, machine learning, natural language processing, and human-computer interaction to mimic the way the human brain works. Cognitive security is the implementation of two broad and related capabilities:

- the use of cognitive systems to analyse security trends and distil enormous volumes of structured and unstructured data into information, and then into actionable knowledge to enable continuous security and business improvement,
- the use of automated, data-driven security technologies, techniques, and processes that support cognitive systems that have the highest level of context and accuracy.

From Compliant to Cognitive

Since the age of the first networks and the hackers who soon followed, we have developed security technology to stop attacks. To date, there have been two distinct eras of cybersecurity: perimeter controls and security intelligence. These serve as building blocks as we enter the third era: cognitive security. Perimeter controls, security that confines (pre-2005): We started with static defences to guard or limit the flow of data, including firewalls, antivirus software, and web gateways. The evolution of information security within the enterprise began as a compliance exercise. The goal was to lock down and restrict access to sensitive information via passwords and a range of access control strategies. Success meant passing an audit. While perimeter defences are still in use, they are not sufficient by themselves for today's environment.

> “ Perimeter defences are not sufficient by themselves for today's environment.

Security intelligence, security that helps you think (2005+): Over time, we progressed to sophisticated monitoring systems that can collect and comb through massive amounts of data to discover vulnerabilities and prioritize potential attacks. This transition led to a focus on real-time information

to detect suspicious activity. Today, security intelligence is the real-time collection, normalisation and analysis of structured data, generated by users, applications, and infrastructures. Security intelligence uses analytics to detect deviations from regular patterns, uncover changes in network traffic and find activities that exceed defined levels. Within a security intelligence infrastructure, analytics are applied to massive amounts of information in an effort to understand company data within context and prioritise day-to-day activities. By determining which deviations are meaningful, security intelligence does not only help detect compromises faster, but also reduces false positives to save time and resources.

Cognitive security, security that understands, reasons and learns at scale (2015+): Built upon security intelligence, which leverages big data analytics, cognitive security is characterised by technology that is able to understand, reason, and learn. A much greater scale of relevant security data is now accessible with cognitive systems that can process and interpret 80% of today's data that is unstructured, such as written and spoken language. After ingesting a corpus of knowledge, curated by experts on any given subject, a cognitive security system is trained by being fed a series of question-and-answer pairs.

> “ Cognitive security is characterised by technology that is able to understand, reason, and learn.

This machine "knowledge" is then enhanced as security professionals interact with the system, providing feedback on the accuracy of the system's responses. A key difference: a cognitive system comprehends and processes new information at a speed that far surpasses any human. Technical defences can now be trained to analyse thousands of research reports, conference materials, academic papers, news articles, blog posts and industry alerts every day. As cognitive systems continue to observe events and behaviours – distinguishing the good from the bad – the ability to leverage integrated defences to block new threats gets increasingly stronger. By helping to make security analysts more effective and accelerating the response to emerging threats, cognitive security will help to address the current security skills gap, bringing heightened levels of confidence and risk control. Cognitive security ultimately plays into a framework built on the basics of traditional security. Security intelligence is not going away; it is a key building block of cognitive security. What the cognitive does is give us a way to triage threat intelligence and detection, and provide actionable information at a speed and scale like never before.

> “ By accelerating the response to emerging threats, cognitive security will help to address the current security skills gap.

Because security intelligence and big data analytics are traditionally focused on structured data, the cognitive element brings an important additional level of understanding to what is going on and how to act. With this full stack, you can have the maximum amount of protection available for your security environment.

Digging Deeper, Going Wider

A single-minded focus on detecting malware, malicious threats, outliers, and anomalies can tend to result in too many false positives. That is the advantage of the multidimensional playing field in which cognitive systems operate. In today's world, the ability to distinguish between black and white is just one aspect of the expertise required for an integrated security infrastructure. There is an increasing amount of grey area, and that is where cognitive comes in. Fortified with heightened levels of intuition, intelligence and insight, cognitive systems are designed to be continuously enhanced

with data and information to help distinguish acceptable behaviours from subtle variations that could signal emerging threats. The result is a broader perspective and a proactive focus on the big picture.

Addressing The Skills Gap

It is not just our systems that are challenged in keeping up with today's security environment; there are challenges on the staff side as well. The number of unfilled information security positions around the world is estimated at 208,000 and is expected to grow to 1.5 million by 2020[5]. Cognitive security can help. Serving as a scalable resource to support human capabilities, cognitive systems can act as extensions to often understaffed security departments. This new dimension is vital because it is no longer enough to keep a close watch on what is happening within your own systems. You need to monitor threats on a global scale in order to prepare for potential attacks. Cognitive can ease the task of the security analyst by providing human-centric communications, such as advanced visualizations, interactive vulnerability analysis, risk assessment, remediation, and possible attribution. Cognitive systems will be able to spot anomalies and flawed logic, and provide evidence-based reasoning. This enables analysts to weigh alternative outcomes to improve decision making.

SPEED RESPONSE WITH EXTERNAL INTELLIGENCE:

When the next Heartbleed hits, people will blog about how to protect yourself from it. Even though a signature is not available yet, there is natural language information online that can help you answer the question. Cognitive systems can crawl to quickly discover how to protect against the next zero-day exploit.

IDENTIFY THREATS WITH ADVANCED ANALYTICS:

Cognitive systems may use analysis methods such as machine learning, clustering, graph mining, and entity relationship modelling to identify potential threats. They can help speed detection of risky user behaviour, data exfiltration, and malware detection before damage occurs.

USE CASES: COGNITIVE UNLEASHED

STRENGTHEN APPLICATION SECURITY:

Cognitive systems can understand the semantic context of your analytics and data, while exploring code and code structures. They can take thousands of vulnerability findings and refine results to a small set of actionable items – and take you to locations in your code where you can fix them.

ENHANCE YOUR SOC ANALYSTS:

Cognitive systems can understand a vast sea of structured and unstructured data to help quickly move the value of a junior analyst from a level 1 to a 2 or 3. Cognitive systems can automate ingesting information – such as research reports and best practices – to give real-time input. Previously, this knowledge and insight could only be obtained from years of experience.

IMPROVE ENTERPRISE RISK:

In the future, cognitive systems could analyse corpuses of interactions, the nature of those interactions and their susceptibility to developing risk profiles for organisations, corporate actions, training, and re-education. Cognitive systems could use natural language processing to find sensitive data in an organisation and redact it.

5 | Report by the Peninsula Press, 2015, based on a number analysis from the US Bureau of Labor Statistics, in the framework of a project of the Stanford University Journalism Program.

The Future: Reversing Cybercrime Economics

Cognitive systems can analyse features, or characteristics, from an enormous set of malicious software – known as malware – in order to detect subtle commonalities. The reason why that is key is that the diversity of malicious software is huge, but cybercrime groups evolve their code, so much of the malware at work today is actually related to other malware. With cognitive systems, we can analyse thousands of features of a suspicious executable file and cluster them to uncover patterns. And without a human ever knowing what those features were, or how or why they matched, the system can identify a pattern that helps discover and classify new malware variants. As the cognitive security community grows, and the viability of new attacks is diminished, cybercrime will enter into a new economic reality. Efforts to develop malware that evades detection will become increasingly complex and costly. According to the Ponemon Institute's 2015 Cost of Data Breach Study, 256 days is the average time it takes organisations to detect advanced persistent threats; and $6.5 million is the average cost of a U.S. data breach. Cognitive security will empower security analysts with the capabilities to find early warnings of potential attacks and significantly speed detection. Cybercriminals will find the payoffs to be harder and harder to achieve. Cognitive computing is driving transformational change by harnessing not just data, but meaning, knowledge, process flows, and progression of activity at a lightning-fast speed and scope. For organisations that embrace cognitive capabilities, the competitive advantage will be significant and far-reaching.

Integration and Expertise for a Cognitive Ecosystem

Integration and expertise are paramount to doing security right. Too many security practices are built on a collection of point products that are not integrated, and do not provide the visibility and actionable intelligence you need to respond quickly. It is not complete integration until your domain capabilities can interact and communicate with one another across your hybrid IT environment, extending beyond your company walls across your entire ecosystem. The right integration can help you get the visibility you need to respond swiftly to security incidents when they occur. Integration allows you to do more with less, which is a fundamental way to address the security skills gap. New threats are discovered every day, which means security expertise and threat intelligence sharing are essential. If you do not have top-grade expertise feeding into a set of solutions and cognition, you are in danger of falling behind. ■



TAURON






We create PROGRESS

24H SERWISANT

Every day we support innovative ideas and develop new opportunities. We invest in technology and care for sustainable development. We work with passion and energy to achieve success. That makes us special.

INNOVATION **PASSION** **BONDS** **RELATIONS**

tauron.pl

ANALYSIS

SECURITY IN THE DOMAIN NAME SYSTEM

MATT LARSON
is Vice President of Research at ICANN, where he leads a team of researchers and oversees the research agenda at this organization responsible for coordinating the Internet's system of unique identifiers. Previously Matt was CTO at Dyn, which specializes in Internet performance, and Vice President, Research at Verisign, where he ran Verisign Labs, the applied research group at Verisign. He is the author of three O'Reilly books on DNS and co-hosts the "Ask Mr. DNS Podcast". You can follow him on Twitter @matthewhlarson.

It is not an exaggeration to state that the Domain Name System (DNS) makes the Internet actually usable. DNS allows people to use human-friendly names and called domain names as identifiers for Internet resources, such as web sites and email addresses. Behind the scenes, DNS quickly translates those names into the IP addresses and other information required by the underlying infrastructure to route traffic from place to place.

DNS has been an astounding success. The protocol, the clients, and the servers that implement it form one of the largest distributed databases, if not the largest, in the world. The DNS database is vast, containing an entry for every device on the Internet that has a name. The contents are distributed across the entire Internet and cooperatively administered by countless organisations.

The Lack of Security in DNS

But as important as DNS is to the operation of the Internet, for a long time security was not a primary consideration in its design. DNS originally had no mechanism to authenticate the origin of data and no data integrity protection.

> "As important as DNS is to the operation of the Internet, for a long time security was not a primary consideration in its design.

When a DNS client sent a query to a server, the client had little choice but to believe the server's response. The protocol did not offer any assurance to a client that the response was actually from the server queried originally.
A client could take some precautions, but ultimately a determined attacker could mount a spoofing attack by impersonating a server and sending a bad answer to a client. Such a spoofing attack is particularly dangerous because of widespread caching in DNS, allowing incorrect information to be redistributed.

Most devices that need to resolve names to IP addresses have a very simple DNS client called a "stub resolver", which cannot navigate the DNS distributed database itself to look up information. Instead, a stub resolver relies on a DNS component called a "recursive name server" to do the lookup. An application, such as a web browser, calls the stub resolver (usually a service provided by the operating system) to resolve names. The stub resolver formulates a DNS query based on the application's request and sends it to a recursive name server. The recursive server sends the necessary queries to track down the answer and return it to the stub resolver, which passes that information back to the application (see Figure 1 for illustration).

Nearly every device on the Internet needs the services of a recursive name server. Most network operators operate these servers for devices on their network, so recursive servers are typically found on every ISP and enterprise network. There are also third-party recursive servers that anyone can use, such as those operated by OpenDNS and Google, just to give two examples. Recursive name

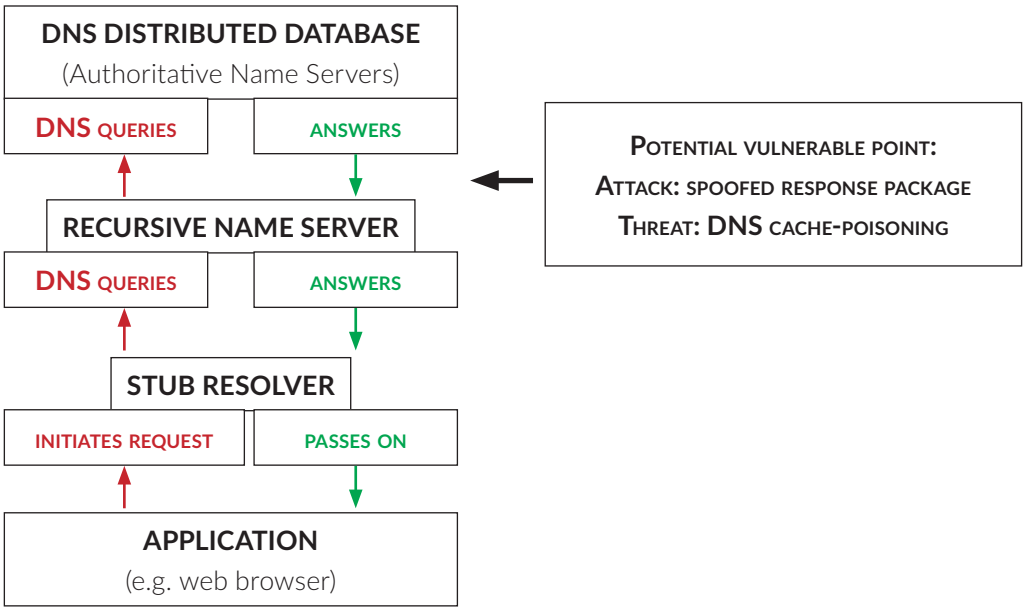


Figure 1. Simplified illustration of the process of resolving names to IP adresses. Source: own contribution

servers are almost always shared by a large number of devices and users. Since they also cache DNS responses they receive to speed up subsequent lookups, recursive servers are tempting targets for spoofing attacks: if an attacker can slip bad data into a recursive server's cache, many people could be affected.

The security shortcomings of DNS, particularly the lack of origin authentication and data integrity, were well known from early in the protocol's deployment, and the engineering community began work on a solution in the early 1990s. The first version of the DNS Security Extensions protocol, or DNSSEC, was published as RFC 2065[1], "Domain Name System Security Extensions", in 1997. The community gained experience with the protocol based on a limited number of implementations and small deployments, almost always in a controlled testing scenario. The DNSSEC specification was refined and revised several times, with major changes and additions in 1999, 2005, and 2008. There was a significant lack of DNSSEC deployment, however. Earlier versions of the protocol were difficult to operate at scale. More serious, however, was a widespread lack of interest: while DNS cache poisoning was a known attack vector, most people believed it was too difficult to be a threat.

Consider an attacker who wants to poison a recursive server's cache with a malicious address for www.example.com. The attacker can send a spoofed response packet hoping that the server will accept it and cache the malicious content. However, a recursive name server will not accept just any response: the response must actually correspond to an outstanding query that the recursive server is waiting for an answer to. The attacker must, therefore, cause the recursive server to send a query for www.example.com, and then send a malicious spoofed response before the legitimate response arrives.

Even if the attacker wins the race and his spoofed packet beats the legitimate response, not just any response for www.example.com will do. The attacker must construct an appropriate response that matches various parameters in the original query. Unless all these conditions are met, the recursive server will discard a response as unsolicited and bogus.

1 | Eastlake, 3rd, D. and Kaufman, C., RFC 2065, *Domain Name System Security Extensions*, 1997, [online] https://www.ietf.org/rfc/rfc2065.txt (access: 09/09/2016)

If the attacker loses the race, the server will process the legitimate response and cache its contents. The attacker's window is now closed: subsequent queries to the recursive server for www.example.com will not cause another query, but instead will be answered from the cache. The frustrated attacker must now wait the duration of the TTL (Time to live) value on the DNS data (also called a record) for www.example.com. The TTL controls how long a recursive server can cache the record, which can vary from seconds to days.
Based on this description of the complexity of a DNS cache-poisoning attack, it is easy to understand operators' feeling of relative safety. Because of the perceived difficulty of a cache-poisoning attack, no recursive server operator believed that they were significantly vulnerable. On top of that, there had never been a significant cache-poisoning attack reported since 1997[2]. The feeling of safety from cache-poisoning attacks led to little motivation to deploy DNSSEC. The cost to deploy was perceived as out of proportion to the magnitude of the threat represented by DNS cache poisoning.

Selected Acronyms

DNS	– Domain Name System
DNSSEC	– DNS Security Extensions protocol
RRSIG	– Resource Record Signature
CA	– Certificate Authority
KSK	– ey Signing Key, sent to parent zone
ZSK	– Zone Signing Key, signing the zone
HSM	– Hardware Security Module
KMF	– Key Management Facilities

That perspective changed dramatically during the summer of 2008. Security researcher, Dan Kaminsky, demonstrated a cache-poisoning technique showing that an attack was far easier than everyone had believed. Kaminsky discovered a way to "run the race" of malicious reply vs. legitimate reply over and over again. No delay was necessary between poisoning attempts, and the attack could be attempted as many times as necessary until successful. However, a full description of the attack is beyond the scope of this article.

> "Security researcher, Dan Kaminsky, demonstrated a cache-poisoning technique showing that an attack was far easier than everyone had believed.

It quickly became clear that there was no easy defence against the attack. While an attacker still had to match certain parameters in a spoofed response for the response to be accepted, there was no penalty for guessing incorrectly. The attacker could try again and again, and the math showed that a determined attacker could eventually succeed in a reasonable amount of time. The only way to address the attack was for the response to include information that could not be guessed by the attacker, but could be verified by the recursive server. A digital signature is exactly that sort of information. Fortunately, a digital signature over DNS data is exactly what DNSSEC provides. The Kaminsky attack motivated renewed interest in DNSSEC deployment.

How DNSSEC Works

Understanding DNSSEC requires some knowledge about how DNS works. The DNS distributed database is divided into regions called zones to allow different parties to manage different portions of the database. The structure of the DNS database is an inverted tree. The tree is inverted because the root is at the top and the branches

2 | In that event, the domain *internic.net* was redirected as a protest. The attack exploited vulnerability in early versions of a particular DNS implementation, which was quickly patched. That attack technique is no longer viable.

grow downward (rather than upward as with a botanical tree). Each level in the DNS tree usually corresponds to a new zone. For example, at the top of the DNS tree is the root zone. Below that are zones for top-level domains, such as eu, pl, and com. Still lower are second-level zones, such as example.com. Each zone is administered separately. The contents of the zones are made available by authoritative name servers, which answer DNS queries about information in the zones they know about, or are authoritative for.

DNSSEC adds data origin authentication and data integrity to DNS using public-key cryptography. DNSSEC is enabled on a zone-by-zone basis, and if DNSSEC is enabled for a zone, the zone is said to be signed. All data in the zone is signed and the resulting digital signatures are stored in the zone as RRSIG records (resource record signature). Each zone has at least one key pair (but usually two, as described below). The public key is published in a special DNS record type called DNSKEY, and the private key signs the zone's contents.

DNSSEC separates signing the data from serving the data, i.e., answering queries. This design allows the private key to be kept secure, for example, on a server behind a firewall or even kept offline, except when in use. Once the data is signed, it can be sent to authoritative servers, which usually sit in a more hostile open environment and are often even run by another organisation altogether as many organisations outsource their authoritative DNS service. But because of DNSSEC's separation of signing and serving, one party can keep the possession of the private key for signing and deliver the signed zone to a third party for serving.

To validate a signature over signed DNS data, one needs to obtain the public key corresponding to the private key that generated the signature. But one must trust the public key in order to trust the signatures it creates. In the X.509 certificate model, a trusted third party certificate authority (CA) vouches for an entity's public key by signing a digital certificate attesting that the specified public key belongs to the specified entity. If one trusts the CA's public key, one trusts the statement represented by the certificate, and thus one trusts the entity's public key.

DNSSEC uses a different model: there are no certificates in DNSSEC. Instead, trust in a zone's public key is derived from the zone's parent[3]. The child zone sends its public key (stored in a DNSKEY record) to the parent zone, which creates a cryptographic hash of the key. The parent publishes this hash in a Delegation Signer (DS) record, which it signs with its own private key. The combination of a DS record in the parent containing the hash of a child zone's public key, along with the parent's signature over the DS record, is the DNSSEC analogue of a digital certificate.

But this design ties the DNSSEC operation of the child zone closely to the parent. Whenever the child wants to change, or roll, its public-private key pair, it must coordinate with the parent to ensure the parent is always publishing a DS record corresponding to the current key used by the child. To avoid this operational dependency on the parent, a zone may have two keys: one key that it sends to the parent and another that it uses to actually sign the zone. The former is called a key-signing key, or KSK, and the latter is called a zone-signing key, or ZSK.
As previously described, each public key for a zone, whether KSK or ZSK, is published in a DNSKEY record. Together, all the zone's DNSKEY records form the zone's key set. While the zone's KSK signs the zone's key set (and only the key set), the signature is published in the zone in an RRSIG record. The ZSK signs all other data in the zone, and those signatures are also published in the zone in RRSIGs. If one trusts a zone's KSK and validates the signature over the entire key set made with

3 | Zones above and below each other in the DNS tree are referred to as parent and *child*. For example, the *com* zone is the parent of the *example.com* zone, which is the child of *com*.

the KSK, then one trusts all the keys in the key set, including the ZSK. Since all other data in the zone is signed with the ZSK, which is now trusted because of the KSK's signature over the key set, all data in the zone can be validated.

A piece of signed DNS data can be validated by starting with a key known to be good and building a "chain of trust" moving downward through the DNS tree, from the trusted key to the signature of the data in question. The known-good starting key is called a trust anchor. The DNS root zone is signed and for most DNSSEC validation, the root zone's KSK is the only trust anchor needed. Starting with the root zone's KSK, one can build a chain of trust through signed zones to validate any piece of DNS data.

For example, consider a recursive name server that has just looked up the IPv4 address of www.example.com from the signed example.com zone. The response includes a DNS type A (address) record for www.example.com, and the corresponding RRSIG record containing the digital signature over that A record. Assuming the recursive name server has the root zone's KSK configured as a trust anchor, the server can build this chain of trust to validate the signature of the www.example.com A record in the RRSIG:

- The chain of trust's starting point is the root zone's KSK, which is trusted implicitly because it is configured as a trust anchor.
- The root zone's KSK signs the root zone's key set, which includes the root zone's ZSK. Using the trusted root zone's KSK to validate the signature over the root zone's key set, the root zone's ZSK is now trusted.
- The root zone's ZSK signs the DS record for com, which includes a hash of the com zone's KSK. Using the root zone's ZSK to validate the signature over the DS record for com, and after verifying that the hash of the com zone's KSK matches the hash in the com DS record, the com zone's KSK is now trusted.
- The com zone's KSK signs the com zone's key set, which includes the com zone's ZSK. Using the trusted com zone's KSK to validate the signature over the com zone's key set, the com zone's ZSK is now trusted.
- The com zone's ZSK signs the DS record for example.com, which includes a hash of the example.com zone's KSK. Using the com zone's ZSK to validate the signature over the DS record for example.com, and after verifying that the hash of the example.com zone's KSK matches the hash in the example.com DS record, the example.com zone's KSK is now trusted.
- The example.com zone's KSK signs the example.com zone's key set, which includes the example.com zone's ZSK. Using the trusted example.com zone's KSK to validate the signature over the example.com zone's key set, the example.com zone's ZSK is now trusted.
- Finally, the example.com ZSK signs the A record for www.example.com. The example.com ZSK is trusted from the previous step and is used to validate the signature over the www.example.com A record, completing the overall validation process.

Administration of the Root Zone's KSK

This description of the validation process illustrates the significance of the root zone's KSK, which is administered by ICANN (The Internet Corporation for Assigned Names and Numbers), a not-for-profit public-benefit corporation. One of ICANN's important roles is performing the IANA (Internet Assigned Numbers Authority) functions on behalf of the global Internet community. The IANA functions include management of the root zone, which includes managing the root zone's KSK. The procedures surrounding the management of this key are interesting and worth describing in more detail.

> This description of the validation process illustrates the significance of the root zone's KSK, which is administered by ICANN.

The root zone's KSK is the "master key" for DNSSEC and is critical to its proper operation. Because of the importance of this key, it must be carefully protected, a responsibility that ICANN takes very seriously. The key resides in a Hardware Security Module (HSM), which can be thought of as a "black box" that stores the key, accepts data to be signed, and outputs the signature. The private key cannot be exported from the HSM, except in highly encrypted form to allow it to be copied to another HSM for redundancy. The HSM is tamper-resistant and will erase the key material if the device is opened or even dropped more than a few inches.

ICANN operates two Key Management Facilities (KMF) to securely store and operate the root zone KSK: one on the east coast of the United States and one on the west coast. The facilities' design specifies seven tiers of security. These tiers are like layers of an onion, ranging from Tier 1, just inside the security perimeter of the shared data centres where the KMFs reside, all the way to Tier 7, the protected storage of the HSM itself where the key is actually stored. The middle security tiers include multiple levels of physical security within the KMF, such as a mantrap to enter and a separate area containing safes for equipment. Access to the various portions of the KMF requires multiple ICANN staff to prevent any one person from using the key inappropriately.

ICANN believes that transparency and openness in administration of the root zone's KSK are vital to increasing the Internet community's trust in the key. The root zone's ZSK is rolled every calendar quarter, so once per quarter ICANN holds a "key ceremony" to use the root zone's KSK to generate signatures over the ZSK for the next calendar quarter. These ceremonies are announced in advance and streamed live on the Internet for anyone interested in watching them. In some instances, interested members of the public have attended the ceremonies as observers.

Another way that ICANN promotes the community's trust in the key is actually involving the community in the key's use. As part of initially signing the root zone in 2010, ICANN put out a call for interested parties to apply to be a Trusted Community Representative (TCR). Fourteen people from all over the world were selected, with seven assigned to each KMF. The procedures that ICANN developed for administering the root zone's KSK require that members of the community be present whenever the KSK is used. At least three of the seven TCRs must be present at a key ceremony in order to use the KSK. Each TCR has a physical key to a safe deposit box inside a safe in the KMF, and inside the safe deposit box is a smart card. The requirement for the TCRs' presence is actually enforced by the HSM itself. During the ceremony, each TCR retrieves his or her smart card, and at least three out of seven smart cards must be inserted into the HSM before the device will sign anything using the root zone's KSK.

Next Step: Rolling the Root Zone's KSK

While the root zone's ZSK changes every quarter, the root zone's KSK has remained unchanged since the root zone was signed in 2010. When the root zone was first signed, ICANN indicated that it would roll the root zone's KSK after five years. No cryptographic key should live forever: just as passwords get changed occasionally, cryptographic keys need to be rolled.

ICANN implements a policy based on the community consensus derived from its bottoms-up, multi-stakeholder approach. As the five-year mark approached, there were calls in the community to investigate rolling the KSK.

ICANN convened a design team comprising DNSSEC experts from the community and the team proposed a plan to roll the KSK. ICANN staff is now in the midst of a project to roll the key, following the design team's recommendations. ICANN does not believe the key is vulnerable, but wants to perform a KSK roll under normal operations rather than in an emergency (such as if the key were believed to be compromised).

> "The most important date is the actual roll itself, when the new KSK begins to be used, which occurs on 11 October 2017.

Assumed to take nearly two years from start to finish, the plan is very conservative because of the critical nature of the root zone's KSK. The most important date is the actual roll itself, when the new KSK begins to be used, which occurs on 11 October 2017.

Any device performing DNSSEC validation has a copy of the root zone's KSK, and that information will need to be updated when the key changes. Some DNSSEC validator software implements a protocol that automatically updates its trust anchors (the automatic update protocol is often referred to by the standards document defining its specification, RFC 5011)[4]. Operators of implementations configured for automatic updates will not need to take any action other than verifying that the trust anchor was successfully updated before the roll. For those operators not running automatic updates, most DNSSEC validator software includes a copy of the root zone's KSK pre-configured either by the software's developer or a downstream packager or integrator, such as Linux distribution maintainers. In that case, as long as the operator is running a recent version of DNSSEC validator software, it should be properly configured with the new key. If the operator has not obtained the new key either by the automatic update protocol or by software upgrade, they will need to manually update their configurations before 11 October 2017.

The current initial phase of the project involves publicizing the roll to two groups: DNSSEC validator operators and DNSSEC validator developers and integrators. ICANN is informing these groups of the upcoming changes and providing resources to help[5].

Conclusion

The addition of origin authentication and data integrity provided by DNSSEC is causing protocol designers to realize that information beyond IP addresses can be stored and retrieved securely with DNS. DNS is now increasingly being used as a secure repository for other kinds of information. For example, the protocol designers in the IETF (Internet Engineering Task Force), an Internet standards body, have recently developed a protocol called DANE (DNS-Based Authentication of Named Entities). When connecting to a server using TLS, the server's public key must be authenticated. Traditionally, this authentication has relied on the X.509 certificate authority infrastructure. But DANE allows a server's public key to be authenticated with key material stored in DNS, and secured by DNSSEC as an alternative to the traditional certificate authority system. This design would not be possible without the assurance provided by DNSSEC. We can expect similar new uses of DNS as DNSSEC allows the protocol to continue to evolve to meet the needs of the ever-changing Internet. ■

4 | StJohns, M., RFC 5011, *Automated Updates of DNS Security (DNSSEC) Trust Anchors*, 2007, [online] https://www.ietf.org/rfc/rfc5011.txt (access: 09/09/2016).

5 | More information about the project is available at https://www.icann.org/resources/pages/ksk-rollover.

POLICY REVIEW

UKRAINE'S CYBERSECURITY STRATEGY AND WAYS TO IMPLEMENT IT

DR MYKHAYLO GUTSALYUK
Mykhaylo Gutsalyuk is a Leading Specialist of the Interagency Scientific Research Centre on Organized Crime Combating of the National Security and Defence Council of Ukraine. He is an expert on combating cybercrime, information security and the implementation of EU legislation in Ukraine. He gained a lot of expertise in computer science and law enforcement, through different positions in the governmental and private sector. Dr Gutsalyuk graduated from the Kyiv Polytechnic Institute, in the Control Systems Department, and has a PhD in Law, from the Kyiv National Academy of Internal Affairs. He is the author of more than 100 publications.

One of the main trends in modern information society is a rapid development of the global computer network (the Internet) and the appearance of a number of new services such as e-government, social networks, e-commerce, e-banking, etc. Modern information technologies create the opportunity for free access to the network in public places, even in remote rural areas. From a technological point of view, the information space is characterised by the complexity of information systems, virtualisation of computer networks, multiplicity of communication, integration of telecommunications and media sectors. Ukraine has a significant potential and a history of functioning as information society. The first electronic computer in the continental Europe was created in Kyiv, in 1951, by a group of scientists led by Serhii O. Lebedev.

Nowadays, Ukraine is an active member of the European digital society, capitalising on the experience of the rest of the world in introducing new technologies. This fact contributes to the equitable integration of Ukraine into the global community. According to the UN rating, E-Government Development Index 2016 (EGDI), Ukraine is ranked 62nd among 193 countries, rising by 25 points compared to 2014 year[1]. At present, information technologies, computer networks, and the Internet are used in all sections of society, including education and science, banking, manufacturing, medicine, law enforcement, and defence, etc. It significantly simplifies the management process of specific areas and the entire sectors of economy, contributing to the democratisation of society and improving the citizens' welfare.

Along with the expansion of information technologies, the number of law violations involving the use of computer technologies as a tool or having computer equipment itself as the subject of the offence has been increasing. Transfer

1 | http://tnijurl.com/unegovernmentindex.

of business to the online regime has attracted the attention of different transnational criminal groups that develop and iTable 1. Evolution of the Ukrainian legal framework concerning cybersecurity issues.liability of information services. It is also a significant obstacle to social development, particularly to the use of Information and Communications Technology (ICT). Today, the most common offences in Ukrainian cyberspace are online shopping fraud and various criminal schemes in the banking sector, including payment cards[2]. At the same time, there are cases of complex cyberattacks on critical infrastructures, masterminded by groups of hackers. As a result of such an attack on the Ukrainian energy industry in December 2015, more than 220,000 users[3] did not have electricity.

Combating cybercrime requires the adoption of new approaches and the development of a proper legal framework in the field of cybersecurity. It also calls for training of special units to combat cybercrime, and taking technical actions to ensure the adequate security level of information resources, especially of critical infrastructure and its assets.

Table 1. Evolution of the Ukrainian legal framework concerning cybersecurity issues.

1994	Criminal liability for the violation of automated control systems is established by the Criminal Code of Ukraine (Article 198-1).
2001	The new Criminal Code of Ukraine includes "Crimes against the use of computers, systems and computer networks and telecommunications" (special section XVI).
2005	Ukraine ratified the European Convention on Cybercrime (signed in 2001).
2007	Set up of the Computer Emergency Response Team of Ukraine (CERT-UA).
2009	The CERT-UA was accredited at the Forum for Incident Response and Security Teams (FIRST).

The National Security Strategy of Ukraine

In recent times, Ukraine's defence sector has been actively reforming itself to keep abreast with the major changes in the foreign and domestic security environment and the emergence of new security challenges, including threats posed by hybrid warfare. As a consequence, the Decree of the President of Ukraine of 26 May 2015 number 287/2015 approved the National Security Strategy of Ukraine that identifies the following priorities to ensure the cybersecurity of the country:

- Creation of a system to ensure cybersecurity, including the establishment of the Computer Emergency Response Team of Ukraine (CERT);
- Development of capacities of law enforcement agencies to facilitate investigation of cybercrime;
- Protection of critical infrastructure and government information resources against cyberattacks; drawing upon the best practices of NATO and the EU member states to safeguard state information resources;
- Creation of a cybersecurity training system in response to the needs of the security and defence sector;
- Enhancement of international cooperation in cybersecurity, and intensification of cooperation between Ukraine and NATO.

2 | Yevgeniya Ivanova, *Nashi IT-zlodei - luchshiye v mire. I kiberkom nuzhno derzhat' marku*, available at http://story.vesti-ukr.com/tr-128-intervyu-o-kiberkopah.

3 | http://biz.liga.net/all/it/stati/3251987-rassledovanie-kiber-ataki-na-ukrainu-kak-virus-slomal-oblenergo.htm.

The Cybersecurity Strategy of Ukraine

In order to create conditions or the safe functioning of cyberspace and its use for the benefit of individuals, society and the state, a separate document named "The Cybersecurity Strategy of Ukraine" (hereinafter – the Strategy) has been developed and approved by the Decree of the President of Ukraine of 15 March 2016 number 96/2016.

> "In order to create conditions for the safe functioning of cyberspace, society and the state, a document named "The Cybersecurity Strategy of Ukraine" has been developed and approved.

Given the current widespread use of information technologies in the defence and security sector, the document was created to tackle the possibility of using cyberattack for terrorist purposes, particularly for violating regular modes of automated processes of critical infrastructure control systems, including the unified automated control system of the Armed Forces of Ukraine. The document identifies factors that increase the threats to Ukrainian cybersecurity, namely:

- The lack of protection of critical information infrastructure and state electronic information resources;
- The lack of effectiveness of the Ukrainian security and defence sector in combating cyberthreats of the military, criminal, terrorist, etc. kind;
- The lack of coordination, cooperation, and information exchange between the entities responsible for ensuring cybersecurity.

The main subjects in charge of cybersecurity in Ukraine are:

- The National Security and Defence Council of Ukraine that, according to the Constitution of Ukraine, coordinates and controls the activities of the security and defence agency strengthening Ukraine's cybersecurity;
- The Ministry of Defence of Ukraine;
- The State Special Communications Service of Ukraine;
- The Security Service of Ukraine;
- The National Police of Ukraine;
- The National Bank of Ukraine;
- Intelligence agencies.

The Strategy determines the following priorities for ensuring cybersecurity:

- Adaptation of a state cybersecurity policy aimed at developing a more secure cyberspace and achieving compatibility with the relevant NATO and EU standards;
- Creation of a national regulatory framework and terminology in this area; harmonisation of legal regulations regarding electronic communications, information and cybersecurity in compliance with international, NATO, and EU standards;
- Development and improvement of information security state control and the system of independent information security auditing; implementation of the best practices and international standards for cybersecurity and cyberdefence;
- Development of international cooperation and support of international cybersecurity initiatives that meet Ukrainian national interests.

In addition, the Strategy pays special attention to the protection of critical infrastructure by focusing on:

- Improving the comprehensive legal framework for the cybersecurity of critical infrastructure;
- Establishing the state register of the critical information infrastructure;
- Providing regulatory requirements

for safeguarding critical infrastructure in cyberspace;
- Ensuring cooperation between entities ensuring the cybersecurity of critical infrastructure; establishing public-private partnership to prevent cyberthreats; responding to cyberattacks and cyber incidents and mitigating their destructive effects, particularly in the situations of crisis, emergency, and martial law, in particular periods;
- Enhancing the capacity of entities fighting cyber terrorism to combat cyberattacks against government electronic information resources, critical infrastructures, as well as identifying and preventing reconnaissance and subversive activities of foreign information services, organisations, groups and individuals against Ukraine in cyberspace.

The National Cybersecurity Coordination Centre

On 7 June 2016, the National Cybersecurity Coordination Centre was founded by the Decree of the President of Ukraine number 242/2016. As a working body of the National Security and Defence Council of Ukraine, the Centre is responsible for the coordination of cybersecurity measures.

> “ On 7 June 2016, the National Cybersecurity Coordination Centre was founded.

The members of the Centre represent the following entities within the Ukrainian security and defence sector in charge of cybersecurity: First Deputies or the Deputy Minister of Defence of Ukraine, the Chief of Defence of the Armed Forces of Ukraine, the Head of Security Service of Ukraine, the Head of Foreign Intelligence Service of Ukraine, the Head of National Police of Ukraine, the Head of the National Bank of Ukraine (by consent) whose jurisdiction embraces the issues of cybersecurity, the Head of Intelligent Service of the Ministry of Defence, the Head of Intelligence of State Border Service of Ukraine, and the Head of State Special Communications Service of Ukraine.

The main tasks of the Centre include analysing the current levels of cybersecurity, results of the reviews of the national cybersecurity system, and the state of preparedness of cybersecurity entities to respond to cyberthreats; implementing state regulations on the cybersecurity of state electronic information resources, personal data (protection of which is set by law), as well as critical information infrastructure; and analysing cyber incidents data concerning state information resources in information and telecommunication systems, etc. The Centre is also assigned to forecast and detect potential and real threats to Ukraine’s cybersecurity, synthesize international experience in cybersecurity, provides information as well as operational and analytical support for the National Security Council on Cybersecurity. In addition, the Centre participates in organising and conducting international and inter-organisational cybersecurity on-the-job training as well as develops relevant guidance documents and recommendations[4].

Implementation of the Strategy

On 24 June 2016, the Cabinet of Ministers of Ukraine approved an Action Plan to facilitate the implementation of the Strategy in 2016. The development of a similar plan for 2017 is currently underway. The implementation of this plan has already brought beneficial consequences for Ukraine’s cybersecurity: In July 2016, with the support of the OSCE, around a hundred of Ukrainian cyber police officers completed on-the-job training to help them tackle (i.e. detect and investigate) different types of cybercrime, including banking scams, human trafficking, child pornography, or DDoS-attacks, etc. The

4 | http://www.president.gov.ua/news.

new units of cyber police work closely with law enforcement agencies in other countries. Recently, they have taken part in joint operations aimed at combating the spread of child pornography, along with the participants from 30 countries. During the operation, 148 persons were found and charged with dissemination of illegal content. During another joint operation with their German colleagues, a hacker was detained after blocking some German websites[5] and demanding 1.5 million euros to restore them. He is now awaiting extradition to Germany[6].

In Ukraine, as in many other countries, the security sector is being actively reformed to counter new threats in cyberspace. An effective response to cybercrime is possible only on condition that there is close international cooperation of law enforcement agencies, private institutions, and civil society. There are many more challenges to ensure the reliability of cyberspace, including the training of judges, investigators, and prosecutors to make them ready for work with evidence related to electronic crime. Having determined the main areas where cybersecurity needs to be strengthened, we will continue focusing on those in our daily work. ■

5 | Since the court case is not over, the names of the websites are not public yet.

6 | http://story.vesti-ukr.com/tr-128-intervyu-o-kiberkopah

PGZ

POLISH ARMAMENTS GROUP

Polish Armaments Group (PGZ) is the leader of the Polish industry and one of the largest defence groups in Europe. It concentrates more than 60 companies (of defence, shipyard, new technologies sectors), achieving annual revenue of circa PLN 5 billion. By making use of the technology Polonisation potential, close cooperation with the Polish scientists and focus on the research & development process, PGZ offers innovative products which enhance Poland's security. In addition, PGZ modernizes and maintains vehicles, airplanes, helicopters, vessels.

MODERN TECHNOLOGIES FOR DEFENCE

www.pgzsa.pl

ANALYSIS

2016: FIRST SEMESTER REVIEW BY SOC

GAWEŁ MIKOŁAJCZYK
is managing, building and growing the Cisco Active Threat Analytics (ATA) Security Operations Centre (SOC) in Krakow, Poland. He holds numerous industry certificates, including CCIE #24987, CISSP-ISSAP, CISM, CISA, C|EH and SFCE. He is a frequent speaker at IT Security events, such as Cisco Live! Europe, PLNOG, EuroNOG, Security B-Sides, CONFidence, Cisco Connect, Cisco Expo and Cisco Forums. Before joining Cisco, he was an administrator of UNIX systems and system engineer at one of the biggest systems integrator in Poland.

The Active Threat Analytics (ATA) team helps organisations defend against known intrusions, zero-day attacks, and advanced persistent threats by taking advantage of advanced big data and machine learning technologies. ATA also manages a complete security technology lifecycle across the IT infrastructure. This fully managed service is delivered by Cisco security experts and a global network of security operations centers. It provides constant vigilance and on-demand analysis 24 hours a day, 7 days a week.

Let us review the threat landscape of the first half of 2016 as seen from the point of view of security operations, researchers and security practicioners. The data we are going to present here is covered in much greater detail in the Cisco 2016 Midyear Security Report, an over 60-page document co-authored by several organisations within Cisco, most notably Active Threat Analytics, Talos Security Intelligence and Research, Security and Trust Organization, Security Research and Operations (SR&O), Advanced Security Research and Government (ASRG), Intellishield Team, Cognitive Threat Analytics, and Lancope and OpenDNS. Today's organisations have reached a tipping point in the development of their IT infrastructure. They want to simplify and update their devices and software to reduce costs in order to build a strong foundation that will help enable their success in the next-generation digital economy. This is the moment to harden security, enable visibility throughout their networks, and help reduce the unconstrained time to operate that adversaries currently enjoy.

> "This is the moment to harden security, enable visibility and help reduce the unconstrained time to operate that adversaries currently enjoy.

1. Mid-2016 Threat Spotlight: Ransomware

Authors of the well-known ransomware brands such as CryptoLocker and CryptoWall took their malware to a new level of effectiveness when they began using cryptographically sound file encryption. Currently, the majority of known ransomware cannot be easily decrypted, leaving its victims with little option but to pay the asking price in most cases. The ransom is typically paid in Bitcoin.

New ransomware vectors are being developed. Today, email and malicious advertising (malvertising) are the primary vectors for ransomware campaigns. However, some threat actors are now exploiting network and server-side vulnerabilities. One interesting widespread campaign that targeted the healthcare industry earlier this year employed the Samas/Samsam/MSIL.B/C ("SamSam") variant, which was distributed through compromised servers. Malicious actors used the servers to move laterally through the network and compromise additional machines. Also earlier this year, the adversaries used an open-source tool, JexBoss, for testing and exploiting JBoss application servers to gain a foothold in the organisations' networks. Once they had gained access, they proceeded to encrypt multiple Microsoft Windows systems using the SamSam ransomware.

Ransomware's evolution aims at self-propagation. For ransomware operators, the SamSam attack represents an evolutionary change from targeting individual end-users to infecting entire networks. Its propagation method is a simple and a highly effective one. Following SamSam's success, it is only a matter of time before adversaries develop faster and more effective propagation methods to maximize the probability of receiving payment. The concept of self-propagating malware is certainly not new – it has been around for decades, in the form of worms and botnets. Many of these threats continue to be pervasive and effective. The features of self-propagating malware that we see in our Security Operations Centers (SOC) include replication to all available drives, file infections, limited brute-force activity, resilient command and control (C&C), as well as the use of other backdoors and vulnerabilities in widely deployed products. Our observations of the evolution of ransomware suggest that the adversaries who develop the next generation of ransomware are more likely to use software with a modular design, i.e. the type of architecture found in many open-source, vulnerability-testing suites. They may also include more "user-friendly" features to monetize the compromised users more effectively.

2. Attack Vectors Landscape: The Client and Server Side

Client-side attacks are generally favoured as they offer greater user engagement; moreover, users tend to be an ultimate weak link in the attack kill chain. In addition, the client side offers ample opportunity for attackers to gain operational space to work. The popularity of PDF and Java as attack vectors continues to diminish. In January 2016, Oracle announced that it would phase out its Java browser plugin, since the browser vendors are proceeding with plans to end support for it. Oracle is now focusing on its plugin-free Java Web Start technology. Yet top exploit kits still rely on Flash: Exploit kits, which have helped ransomware to become such a prominent threat, still continue to make use of Adobe Flash vulnerabilities. In the recent examination of the popular Nuclear exploit kit, Cisco researchers found that Flash accounted for 80% of successful exploit attempts.

Exploit Kits Use Tor as an Encrypted Channel

Exploit kit (EK) developers are always on the lookout for ways to evade security defences, and they are very creative in their efforts. One example we have recently noticed involved the Nuclear exploit kit. The kit, which typically drops variants of ransomware, was observed to deliver a variant of an anonymous

communications client, Tor. This approach appears to be a method for hiding the eventual malicious payload, and making malicious activity more difficult for defenders to track.

Global Spam Volumes Stay Stable

To approximate spam traffic worldwide, Cisco collects telemetry samples from its email appliances, indicating the impact of policy decisions coded into email appliances and gateways, that is emails that are blocked or marked as unknown. Spam email is frequently used as an attack vector, especially for ransomware. According to our examination of email traffic, spam volumes remained steady from December 2015 to May 2016. Spam traffic from Brazil showed spikes in spam in January and March 2016. These increases are attributed to the activity of a large spam botnet at that time.

Attackers Moving to HTTPS Complicates Defence

Between September 2015 and March 2016, Cisco security researchers observed a fivefold increase in the HTTPS traffic related to malicious activity. To identify this trend in the use of HTTPS, we tracked 80 malicious campaigns across eight threat categories, over a 16-month period. The rise in the HTTPS traffic can largely be attributed to ad injectors and adware. In that period, we observed that a number of malware families began switching to HTTPS:

- Gamarue/Andromeda, a multipurpose botnet
- Necurs, an information-stealing botnet
- Miuref/Boaxxe, a click-fraud botnet
- Ramdo/Redyms, a click-fraud botnet
- Data-exfiltration Trojans

One fallback strategy for defenders is to use blacklists (which list all known malware);however, this method is not only prone to error and not granular enough to be effective, but also manual and time-intensive.

Hot Business: Malvertising-As-A-Service

The malvertising-as-a-service trend is similar to domain squatting (profiting from selling or using domain names that users would be likely to associate with legitimate businesses and well-known brands). By directing traffic from those domains, they facilitate malware distribution without playing a direct role in delivering threats. One campaign that appeared in October 2015 redirected users to exploit kits, including Angler and RIG, which delivered different payloads. Many of those were ransomware variants like TeslaCrypt and CryptoWall. Users were tricked by a malicious advertisement that spoofed a gambling site. A link to JavaScript was buried in the code behind the ad. That link took users to an Angler EK landing page, but there were other redirections as well, including iFrames. The emergence of this new approach to distributing malvertising is another indicator that the shadow economy is becoming more mature and industrialized. We expect the malvertising-as-a-service trend to grow as more cybercriminals look for efficient ways to infect large numbers of web users through legitimate sites and at the same time evade detection.

Time to Patch – Between Availability and Implementation

Despite the availability of patches, many users still do not download and install them in a timely manner. The gap between the availability and the actual implementation of such patches is giving attackers an opportunity to launch exploits – that is, time to operate within a network that could have been blocked with a simple software patch.

“ Despite the availability of patches, many users still do not download and install them in a timely manner.

The malicious actors could start their path to exploitation even before vulnerability has been publicly disclosed. Therefore, closing this gap is crucial for effectivedefence. By studying the installations of browser software on end points used by Cisco customers, we can see the value of automatic updates.

Having instituted a strong opt-out policy, Google Chrome web browser shows that 75% to 80% of users are using the latest version of the browser, or are one version behind. Google makes it increasingly harder to run old versions of its browser. While studying installations of Java software on end points used by Cisco customers, we have detected indicators of compromise (IOCs): one-third of the systems examined are running Java SE 6, which is being phased out by Oracle; the current version is SE 10. For Microsoft Office, across the three major versions with significant adoption, the breakdown by percentage is roughly 28-52-20. We would expect to see most of the population of a major version operate on the newest service pack version, but when looking at Office 2013/version 15x, the three major security update points we divide by are split almost evenly.

Aging Infrastructure Problem – Cisco devices

We wanted to examine a sample set of Cisco devices to determine the age of known vulnerabilities that are running on the Internet infrastructure (routers and switches). Our sample consisted of 103,121 Cisco devices on the Internet (observable installations with known CVEs, dating from 2002–2016). Each device was running, on average, 28 known vulnerabilities. The devices in this sample had been running known vulnerabilities for an average of 5.6 years. More than 23% of these devices had vulnerabilities dating back to 2011. Nearly 16% had vulnerabilities that were first published in 2009. And almost 10% had known vulnerabilities older than 10 years.

Is Grass Greener Elsewhere? Apache and OpenSSH

Cisco researchers examined vulnerabilities in a popular software infrastructure to determine whether organisations were more diligent about patching known vulnerabilities in these products. Our sample of more than 3 million installations with vulnerabilities included a wide range of products, but the majority were either Apache httpd (885,918) or OpenSSH (704,630). The average number of known vulnerabilities for these was nearly 16. According to our research, organisations using web-server software have been running known vulnerabilities for 3.9 years, on average. Thus, it is critical to prioritise the problem of aging infrastructure and systems. This is not only about patching old vulnerabilities, but also assessing the overall strength and cyber-resilience of deployed infrastructures and systems.

Time To Detection – The Cybersecurity Arms Race

"Time to Detection", or TTD, can be defined as the window of time between a compromise and the detection of a threat. This time-window is determined using opt-in security telemetry gathered from Cisco security solutions deployed worldwide. Since the end of 2014, we have been tracking our progress in lowering the TTD. Mid-2015, we have reported that the median TTD was about two days (50 hours). By October 2015, Cisco had significantly reduced the median TTD to about 17 hours. For the period from December 2015 to April 2016, the median TTD was even lower – about 13 hours, which is the weighted average of the five medians for the period observed. Our median TTD is far below the industry estimate of 100–200 days, and we continue to accelerate our ability to detect a wide number of threats. There are a number of peaks and valleys along the line, which are evidence of the "arms race" between attackers and defenders evolving their techniques.

3. A Look Forward Into the Late 2016

As long as attackers are permitted an unconstrained time to operate, they are likely to succeed. But if an organisation can limit adversaries' time and opportunity to lay the foundation for and carry out an attack, they are forced to make decisions under pressure that place them at a higher risk of becoming known and taken down. Based on the observations made by our SOC in the first half of 2016, let us put forward a few security recommendations organisations may employ today to build their first line of defence. They will help impede the opportunity for lateral movement and propagation, and reduce adversaries' time to operate.

> "As long as attackers are permitted an unconstrained time to operate, they are likely to succeed.

1. Segmentation: Organisations can take advantage of well-known network segmentation techniques to stop or slow down the lateral movement of self-propagating threats as well as to contain them. There are multiple components that organisations should consider, such as:

    a. VLANs and subnets for logically separating access to data
    b. Firewall and gateway segmentation
    c. Host-based firewalls with configured ingress and egress filtering
    d. Application blacklisting and whitelisting
    e. Role-based network share permissions (with least privilege)
    f. Proper credential management

2. Backup recovery: In a ransomware scenario in which local backups are deleted, removed, or otherwise made inaccessible by attackers, off-site backups are often an organisation's only hope for restoring service without paying the ransom. How often backups are sent off-site determines how much data, if any, would be inaccessible or lost.

3. Browser infections monitoring: Behavioral analytics tools and collaborative threat intelligence are critical resources for defenders in remediating these types of threats. Educating users to alert security teams to an increase in pop-up ads and other unwanted advertising is also vital for defence.

4. Routine Patching Lifecycle: Organisations need to move beyond "checking off the boxes" approaches that are no longer sufficient for modern threats. A "security first" approach should be developed. For example, security professionals should periodically check for the presence of unexpected system or administrator accounts, using the tools available to them. They should also log and analyze all network communications for malicious traffic, and review such suspicious traffic for IOCs. Leaders should provide the tools that are needed to conduct such in-depth investigations. In addition, they should ensure that the environment is up to date by incorporating a routine patching lifecycle with the most recent patches delivered to operating systems and commonly used software, where threat actors tend to find and exploit weaknesses.

5. IOCs are not Threat Intelligence: We are observing that organisations can spend millions of dollars on lists of Indicators of Compromise (IOC) that are marketed as threat intelligence. In many cases, the reliance on IOCs can create false assumptions that the organisation may be secure and free from attackers. Threat intelligence is data that has been converted into actionable information through

an understanding of the context in which that data was produced. Threat intelligence comes with the targeted "what to do next because of what the data says". Data without this context is not useful enough.

Conclusion

Raising the difficulty for cybercriminals by pushing them to continuously evolve their malware is one strategy for reducing their time to operate. The more they need to adapt, the more likely they are to leave artifacts that will ultimately lead to their identification, no matter how hard they try to evade detection and cover their tracks. This is why it is critical to measure Time to Detection (TTD). If defenders do not know where they stand with their ability to detect threats, they cannot improve. TTD and TTP (Time to Patch) should be applied as key performance indicators. This will enable the SOC teams to embrace the techniques that constrain attackers and force them to change strategies. As always, the organisations and end users play an important role in helping reduce the time that threat actors have to operate. For enterprises, there has perhaps never been a better time – or a more urgent need – to improve security practices, than it is now. ■

ANALYSIS

CYBER IMPLICATIONS OF TECHNOLOGY TRENDS: THEIR IMPACT ON CRITICAL BUSINESS INFRASTRUCTURE

JAKUB BOJANOWSKI
Partner leading Deloitte services related to Cyber, IT audit, internal controls and business resilience. Mr. Bojanowski acts as business advisor to enterprises significantly relying on Information Technology (financial services, telecommunication, infrastructure). Within the cyber domain, he focuses on strategic advisory and managing cyber risk on management board and corporate level. He has graduated in Computer Science at the University of Warsaw and attended Advanced Management Program organized by the IESE Business School (University of Navarra).

Protecting critical infrastructure against cyber risks was easy 10 or 15 years ago. Industrial systems were based on a closed infrastructure, and could be managed only from the administrator console, physically protected in the "control room". The world today is different – industrial systems cannot be considered closed infrastructures anymore. Technology advances and new ideas focused on increased operability, allow IT systems to connect to the Internet of Things (IoT) where miscellaneous technical devices generate and gather detailed diagnostic data exchanged through LAN/WAN servers for the purpose of an in-depth analysis, or just in case ("for future use")[1]. The "old-fashioned" administrator or operator console has been replaced by a PC, a workstation or a tablet and the systems once available to a closed circle of trusted administrators or technicians have become accessible to all employees or, in the worst-case scenario, to the Internet users all over the world.

The problem is that IT security solutions implemented in typical IT business applications cannot be easily adopted for industrial control systems. The traditional security approach may by inadequate or insufficient in a hybrid computer environment, founded on the interoperability of business applications, industrial systems, and the IoT technology. Traditional IT security is based on the credentials of system users ensured by a unique (not shared) user ID, passwords, and access rights. Technological advancements (biometrics, one-time passwords, and sophisticated encryption) make these traditional solutions more effective and easier to use, but they do not change the fundamental paradigm of security being associated with the identity of the system user. Unlike generic business applications, industrial systems are depersonalized by nature. Meters, probes, or any other IoT devices are shared by the entire infrastructure and operate 24/7 without human intervention, so there is no "user" who should be accountable for ensuring system' security. By definition, critical infrastructure needs to maintain 24/7 business operations. This illustrates the importance of having a vigilant security strategy, one that proactively looks for security gaps and anticipates malicious acts to prevent unplanned downtime.

An operator of critical infrastructure should be aware of their security risk profile and increased risk exposure; they should also take into account the fact that adding any new network link or any new IoT device opens up an opportunity for malicious action and new risks[2]. Of course, stopping innovation and keeping industrial systems in a separate environment is not a sustainable strategy either. Security and privacy concerns can be used temporarily to undermine any initiatives focused on new business opportunities or built on emerging technologies, but cybersecurity does not have to impede

1 | *Deloitte Review: Safeguarding the Internet of Things*, Deloitte, 2015.

2 | *Tech Trends 2016 - Innovating in the digital era*, Deloitte University Press, 2016.

innovation. Leading organisations are managing security risks successfully and are even able to turn the understanding of security risks to their advantage. The first step towards adequate security design is to understand the limitations of technology as well as the risk associated with the IoT technology and the risk of connecting industrial systems to corporate networks.

Retrofitting

Large organisations already operating industrial systems often consider adapting existing sensors to the IoT technology. In a typical scenario, old technology sensors have already been deployed on a significant scale, so the reuse of the existing technology ("retrofitting") can be much more economical than developing new, purpose-built technologies and then replacing all existing system components. Retrofitting may be a key enabler for the IoT strategy, but, when doing so, companies need to understand that there may be potential security, performance, and reliability implications, especially when legacy assets are forced to play out scenarios for which they were not originally designed. Many of the sensors already in place were not intended to be connected to a more generally accessible network. Some of the obsolete system components will not be ready for technological upgrade and may need to be reengineered or replaced by purpose-built solutions. Unlike traditional solutions, which fed data from sensors to a secure central system, the IoT functionality makes information move in all directions, with the back-end system now aggregating and analysing all the data. With so many more points of communication, shared system accounts and passwords are no longer adequate: if a malicious actor were able to break into such a system account, he or she could steal sensitive instrumentation data from anywhere in the system or launch a denial-of-service attack, devastating plant operations. So eventually, retrofitting acceptable on smaller scale may cease to be a viable option from a security standpoint.

Given the rapid pace of innovation, many devices will likely become physically incapable of being upgraded to protect against the latest threats, thus rendering the devices outdated and vulnerable to threats.

Interoperability

The interoperability of industrial systems and related security threats is worth a broader discussion as it is very much an overlooked issue. A common feature of many IoT deployments is the creation of an ecosystem that can include many different organisations or stakeholders. In most cases, a typical IoT solution has more than one user: a service company scheduling maintenance, a supplier delivering raw material just-in-time, a client waiting for the delivery of a finished product, or a solution vendor calculating licence fees for technology. All parties generate data and a large part of the value of IoT deployments is based on the ability to aggregate these data; yet data are generated in different formats, and sensors connect to different networks via different communication protocols. The lack of a single, generally accepted standard governing the functioning of IoT-enabled devices is, therefore, a frequent barrier to the interoperability required to realize the IoT deployments that many envision. The need for such standardisation is evident; yet in the meantime companies can find themselves falling back on ad hoc solutions to create the interoperability that a given IoT solution needs. Unfortunately, even where standards have been adopted, different companies in the same supply chain may well adhere to different standards. Due to the lack of unified standards for data exchange, operational details for data ownership and data exchange need to be agreed on a case-by-case basis and the interoperability of newly designed solutions needs to be defined and agreed by all players.

Ecosystems

The pace of growth of IoT popularity adds another layer of complexity into the security landscape. Industrial systems will no longer be static, with new functionalities and new IoT components being added to the solution either by the company itself or its business partners. In no time, a pilot solution started on a relatively small scale could develop into a complex ecosystem of multiple, hybrid IoT systems where originally established responsibilities for security are no longer relevant. Since IoT-enabled processes and systems extend beyond the home organisation, company's information flows across multiple external devices and databases, each under the control of a different third party. These third parties, however, may not recognize that their secure, vigilant, and resilient strategies – or lack thereof – have implications for the systems of every other stakeholder: the chain is only as strong as its weakest link.

It could be a mistake to assume that partners –less likely customers – should or will take responsibility for maintaining data confidentiality and guarding against breaches. Enterprises should consider acting as being on their own, and rather than presume a shared responsibility for security with their business partners, review the responsibilities of all the stakeholders that touch the data in each of the value loops. Assessing potential risks at each point and making sure stakeholders are aware of those risks can help make a solution more secure. Once each player has established where its responsibilities begin and end, companies develop and maintain clear accounting within the IoT ecosystem and can remain vigilant for threats.

Understanding the Data

More information creates more possibilities to create value: this is the promise of the IoT. On the other hand, it also creates new liabilities and new risks. As technologies improve, so do the scale, scope, and the frequency of data collected. With the cost of data gathering and data storage going down, companies start to collect more data than they can currently consume, building data repositories for future applications. When dealing with such tremendous volumes of data, it is only too easy for relatively small, virtually unnoticeable thefts to pile up until they amount to a veritable fortune. The quantity and variety of information companies collect can make it difficult for them to know if their data have been breached – a situation exacerbated by the fact that much of companies' data may be held by third parties, making them even more difficult to safeguard.

The quantity and variety of data collected via the IoT combined with the fact that so much of that data is now available to third parties can make it difficult for companies to know if their data has been breached. Companies can address this threat by developing a deep understanding of the data they possess and combining this knowledge with analytics to measure against a "normal" set. By establishing a baseline of what "normal" looks like, they can more readily and reliably identify possible abnormalities, triggering further investigation.

Key Takeaways

Regardless of new challenges, companies can still remain secure, vigilant, and resilient by taking several steps to safeguard their ecosystems and the data they create:

- Contribute to defining standards for interoperability. Adhering to one standard only or actively getting involved with consortiums to develop a set of standards can help ensure that devices within a network can all communicate and work together safely and effectively.

- Use purpose-built devices or add-ons, rather than pre-IoT solutions. Companies should strongly consider entirely new, secure technologies designed specifically for the IoT. If

this is impossible, any add-ons used to retrofit the old devices should include purpose-built cyber security measures.

- Develop a clear assignment of responsibilities for the players in your ecosystem. Take the assessments of all stakeholders to understand potential risks at each point and make sure that stakeholders are aware of those risks. All parties in the IoT environment must know where their responsibilities begin and end

- Establish a baseline of data. Viewing IoT systems more broadly and monitoring environmental attributes such as usage, location, and access would better enable enterprises to distinguish what is normal and what constitutes a suspicious aberration. This enables enterprises to take appropriate and effective action when data do stray from the norm.

- Institute data governance. Enterprises should consider playing a stronger governance role by defining which data to secure, what it means to be sufficiently secure, and, by extension, which products meet that goal. Guidance around how data can be securely collected, used, and stored can help prevent unwanted breaches and prevent a risk event from snowballing into something larger. It can also help draw lines of responsibility in the event of a breach.

- Create loosely coupled systems. Ensure devices within an ecosystem are loosely coupled and resilient, so that the failure of one device does not lead to a widespread failure.

The prospects for creating and maintaining seamless and secure critical infrastructure integrated with the IoT technology may seem daunting, considering that vulnerabilities exist on all sides, but progressive cyber risk professionals are open for the challenge. The security of IoT solutions cannot be built ad hoc and need to be based on the understanding of organisational operations and the knowledge of multi-layered cyber risk management techniques, creating offerings that are secure, vigilant, and resilient. It must be integrated into the design process and the approach must balance functionality, time to value, and underlying security, privacy, regulatory, and compliance needs. ■

Security and guaranteed supplies

Diversification of supply sources is the national energy security and our customer's comfort.

We know that the different resources and investments in new projects have impact on the stability of supplies. Therefore, our strategic aims concern increase of oil and gas extraction. Security and quality are paramount value for us.

PGNiG

ANALYSIS

THE CYBER FRONTIER: DIGITALIZATION OF THE GLOBAL SOUTH

NIELS NAGELHUS SCHIA
is a senior research fellow at NUPI (Norwegian Institute of International Affairs). He is a former fellow of the NSSR (New School for Social Research) and holds a PhD degree in social anthropology from the University of Oslo. His current research focuses on cybersecurity, cyber capacity building in developing countries and emerging economies, Internet governance and collaboration between states and non-state actors. He has acted as an adviser to governments and international organizations and he is a former Fulbright scholar and head of the scientific committee for the annual Fulbright award in Norway.

Introduction

Instead of adding to the substantial literature on digital dividends and the Global South, this article examines a related but less-studied issue: the new societal vulnerabilities emerging from digitalization in the Global South. There is broad agreement about the need to bridge the gap between the connected and the disconnected, but the pitfalls are many, especially concerning cybersecurity[1] – a topic often neglected, also in the recent World Bank report Digital Dividends[2]. This contribution is an attempt to redress these shortcomings, using an analysis of the cyber frontier to highlight cultural (trans)formation and continuity[3]. By the "cyber frontier" I mean the interface encompassed by digitalization, between local and national polities in the Global South and large-scale global forces. The frontier perspective thus highlights digitalization as a process in which polities and communities are produced locally, and become (trans)formed through their entanglement with external and digital connections.

The cyber frontier perspective serves to explicate that the Global South's participation in digitalization is not simply a matter of joining cyberspace.

1 | Cybersecurity is closely interlinked with the security of cyberspace; being broadly understood, it involves a multitude of actors in this text. The linkage between cybersecurity and national security is well established and uncontested. Cybersecurity in the technical sphere refers to a: "a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access, in accordance with the common information security goals: the protection of confidentiality, integrity, and availability of information", in: Cavelty M. D., *Cyber-security and private actors*, in Leander A. and Abrahamsen R. (ed.), *Routledge Handbook of Private Security Studies*, Routledge, 2015, p.89. In the national setting it refers to "the security one enjoys in and from cyberspace" (ibid: 91).

2 | World Bank, *World Development Report 2016 - Digital Dividends*, World Bank Group, 2016, available at: http://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

3 | The term "cyber frontier" is inspired by Igor Kopytoff's analysis of "the African frontier", see Kopytoff I. (ed.), *The African Frontier – The Reproduction of Traditional African Societies*, Indiana University Press, 1987.

On the contrary, it is a matter of selective forms of global connection in combination with disconnection and exclusion. Firstly, I contextualize security concerns by describing the trajectory of digitalization in the Global South and how it diverges from that of the more industrialized countries. Selected empirical snapshots are presented, showing the current situation in several countries of the Global South.
I then explore how "technological leapfrogging" can create new and unique societal vulnerabilities. By linking digitalization with security and economic growth, cybersecurity is seen in connection to development assistance and the implementation of the UN Sustainable Development Goals (SDGs). Finally, I hold that this triple knot represents an opportunity for donors such as the EU to foster new types of actions building on a continued engagement in the Global South.

Background

Digital technology underpins most of the social, economic, and political development goals of donor countries and international organisations today. Promoting, cultivating, and encouraging growth and stability in recipient countries through digitalization and capacity building on matters of cybersecurity will play an important role in the future foreign-policy considerations and government programmes[4].

This article identifies and draws on three main reasons why capacity building will be increasingly important with regard to the cyber frontier and the Global South: 1) Access to cyberspace is essential to social, economic, and political stability, so the importance of capacity-building measures and programmes for regional stability will grow. 2) Countries in the Global South are becoming hosts to the infrastructure and actors behind malicious cyber activities. Thus capacity-building measures are also important for enhancing national security, and responding to cyberthreats in donor countries. 3) The international debate about Internet governance is becoming more and more politicized. Many recipient countries hold "swing state" positions in this political landscape, and their influence and importance are likely to grow[5]. The cyber frontier seems set to become an increasingly significant arena for international diplomacy.

However, Information and Communication Technology (ICT) is nothing new. The first undersea telegraph cable (under the Atlantic Ocean) was laid in 1858 by the Atlantic Telegraph Company. The International Telecommunication Union (ITU) was founded in 1865, and became a UN agency in 1947. The ARPANET (predecessor of the Internet) was created in 1969; the first email was sent in 1971; the first Internet worm or malware, the Morris worm, was detected in 1988; and in 1993, the Internet and the World Wide Web were made publicly accessible and free. Although information and communications technology has been around for almost half a century, digitalization and cyberspace represent a fairly new field in international politics (global economic, security, and human rights agendas), and an even more recent addition to the field of development assistance.

In 1999, the first UN resolution addressing cybersecurity was adopted, marking the starting point for a multilateral, intergovernmental effort to deal with cybersecurity. The first UN resolution pertaining to digitalization and development assistance came in 2001, when the General Assembly decided that a World

4 | Some donors have established models for Cyber Security Capacity Building (CCB); see for instance Muller L., *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities*, NUPI Report no. 3, 2015, Norwegian Institute of International Affairs. CCB was initially more concerned with economic issues, followed by international security agendas and human rights. The development context is the latest addition to this field (see Klimburg A. and H. Zylberberg, *Cyber Security Capacity Building: Developing Access*, NUPI Report no. 6, 2015, Norwegian Institute of International Affairs, p.5).

5 | See ibid, and Schia N. N., *Teach a Person how to Surf: Cyber Security as Development Assistance*, NUPI report 4, 2016, Norwegian Institute of International Affairs.

Summit on the Information Society (WSIS) should be held. The first meeting was held in Geneva in 2003, the second meeting in Tunis in 2005; these were followed up by a WSIS+10 in New York in 2015. Because the goal of the first summit was to provide a foundation for an information society for all, this meeting had implications for development politics as well[6]. In 2004, the Partnership on Measuring ICT for Development was launched as a multi-stakeholder initiative to improve the situation in the Global South. In 2005, the second WSIS meeting held in Tunis emphasized implementation and financing mechanisms, as well as Internet governance. Multiple stakeholders broadly supported the outcome resolution of the Geneva and the Tunis meetings. Since then, and particularly in the last five years, the pace of policymaking has increased rapidly. Highways for policymaking have been produced, especially as regards cybersecurity, cybercrime and Internet governance. Now the cyber and development highway also seems to be gaining momentum. In 2015, the WSIS+10 High-level meetings issued recommendations on how to proceed so as to further connect countries in the Global South, and called on all "governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders to integrate information and communication technologies (ICTs) in their implementation approaches to the SDGs"[7].

The 2030 agenda for the SDGs was designed to combat poverty, inequality, and climate change. These overarching goals, further specified into 17 goals and 169 targets, have been seen in conjunction with the spread of new technology[8]. At the cyber frontier, digitalization is contributing to growth and development through increased productivity, by providing public and private services, and promoting new economic and social opportunities for people living in the Global South. The connections between technology and growth have been confirmed through statistics on the use of information technology, and the extent to which countries are connected correlates with increases in GDP[9].

Since 2000, the cyber frontier has gained new terrain. There has been a considerable increase in connectivity, creating new tools for economic growth and social development – and there is no reason to believe that this trend will not continue. According to UN estimates[10], the number of mobile phone subscriptions increased from 2.2 billion in 2005 to 7.1 billion by 2015. Furthermore, 3.2 billion people (of whom 2 billion are from the Global South) were online by the end of 2015 and another 500 to 900 million people are expected to join the global online population by 2017[11]. A GSMA report has estimated that there were 557 million mobile-only subscribers in Africa in 2015[12]. With 46% of the population connected to the mobile market, Africa has become the second largest, yet least penetrated, mobile

6 | In all, 175 countries were represented, together with international organisations, the private sector, and civil society at the meeting in Geneva, where they endorsed the Geneva Declaration of Principles and Geneva Plan of Action, adopted 12 December 2003.

7 | WSIS (World Summit on the Information Society), *Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes*, 2015, point 17, available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN95707.pdf.

8 | See for instance Global Commission on Internet Governance, *One Internet*, 2016; op. cit. World Bank 2016; Bildt C., *Development's digital divide*, Project Syndicate, 2015, available at: http://www.project-syndicate.org/commentary/sustainable-development-goals-digital-divide-by-carl-bildt-2015-08.

9 | Op. cit. World Bank, 2016, p.3.

10 | United Nations, *United Nations General Assembly's Overall Review of the Implementation of WSIS Outcomes*, 2015, p.7, available at: http://www.un.org/pga/70/wp-content/uploads/sites/10/2015/08/2015_October_09_World-Summit-on-Information-Society.pdf.

11 | McKinsey & Company, *Offline and falling behind: Barriers to Internet adoption*, 2014, p.2, available at: http://www.mckinsey.com/industries/high-tech/our-insights/offline-and-falling-behind-barriers-to-internet-adoption.

12 | GSMA, *Number of unique mobile subscribers in Africa surpasses half a billion*, Press Release, 2016, available at http://www.gsma.com/newsroom/press-release/number-of-unique-mobile-subscribers-in-africa-surpasses-half-a-billion-finds-new-gsma-study/#.V5iNQqP3VVw.twitter.

market in the world. GSMA has also estimated that 25% of these subscribers have already gone over to mobile broadband (3G/4G), and expects the figure to rise to more than 60% by 2020. Furthermore, the number of smartphone connections in Africa is expected to triple, from 226 million in 2015 to 720 million by 2020. These technologies are being adopted at such a pace that they are also reaching people who remain below the poverty threshold. For them, digitalization represents an entry ticket to formal networks where they can communicate, transact, access basic financial services, obtain information, and demand their rights and recognition. However, concurring with UN estimates, the World Bank has pointed out the number of people in the world still untouched by the digital revolution:

> *"Only around 15 percent can afford access to broadband Internet. Mobile phones, reaching almost four-fifths of the world's people, provide the main form of Internet access in developing countries. But even then, nearly 2 billion people do not own a mobile phone, and nearly 60 percent of the world's population has no access to the Internet. The world's offline population is mainly in India and China, but more than 120 million people are still offline in North America [...] In Africa, the digital divide across demographic groups remains considerable. Women are less likely than men to use or own digital technologies. Gaps are even larger between youth (20 percent) and those more than 45 years old (8 percent)[13]."*

Furthermore, almost 75% of the offline population is located in 20 countries; 64% of these people live in rural areas, and 50% have incomes below the poverty line average in their countries. While close to 100% of the online population can read and write, around 28% of the offline population is illiterate[14]. Connections have been made between the WSIS+10 and the SDGs, such as action lines for achieving these goals through digitalization[15]. These initiatives have drawn considerable international attention to this agenda, with digitalization increasingly becoming a precondition for sustainable development. Indeed, digitalization has the potential to become a major tool for development to billions of people living in the Global South[16].

Donor countries and international organisations seize on digitalization as an opportunity for fighting poverty. However, digitalization in countries that suffer from the lack of development, poor governance, and poverty may provide a new breeding ground for organised crime, terrorism, and cybersecurity challenges: a new and threatening dimension of social vulnerability follows in the wake of the development opportunities offered by the digital revolution. Baseline studies have demonstrated the gap between the development goals and intentions in donor policies, and digital vulnerability and cybersecurity in developing countries[17]. To be sustainable, digital development will also have to be concerned with digital security. This, in turn, will require core development assistance focused on improving the analogue foundations for digital technology, including knowledge, information, education, employment, and institutions.

1. Digital Dividends in The Global South

The new goal of eradicating extreme poverty in the course of the next 15 years has now been endorsed by the UN through the SDGs. Some claim that it will be possible to achieve this, because

13 | Op. cit. World Bank, 2016, pp.6-7.

14 | Op. cit. McKinsey, 2014, p.3.

15 | See WSIS, *Advancing Sustainable Development through Information and Communication Technologies: WSIS Action lines enabling SDGs*, 2015, available at https://www.itu.int/net4/wsis/sdg/ Content/wsis-sdg_booklet.pdf and op. cit. WSIS, 2015a, point 4.

16 | Op. cit. Bildt, 2015.

17 | See studies for Myanmar: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Myanmar.pdf and Tanzania: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Tanzania.pdf

the Global South is fundamentally changing due to the connectivity made possible by digital networks. Nevertheless, achieving faster growth, more jobs, better services, and broader benefits will be challenging. In the following, I group the challenges that obstruct the realization of digital dividends at the cyber frontier under two headings: weak technological environment, and poor network infrastructure and urban-centred digitalization.

1.2 Weak Technological Environment

The need to build the correct environment for technology before businesses can begin to thrive and then reap the benefits of digital connectivity has been emphasized by international organisations and policymakers[18]. Research has pointed in a similar direction, as seen in the study by Klimburg and Zylberberg and the Dalberg Report[19]. Drawing on a survey of more than 1,300 businesses, 1,000 small and medium-sized enterprises, and extensive interviews in Ghana, Kenya, Nigeria, and Senegal, the Dalberg Report describes the digitalization of these countries as a work in progress, with potentials still largely untapped. It further identifies "core infrastructure" and "conditions for usage" as the two key pillars of a well-functioning Internet economy[20]. Core infrastructure requires an environment with affordable mobile and Internet access – but also with electricity, skills, knowledge, education, and awareness of corruption. Establishing such an environment hinges on various conditions for usage, such as costs, education, and the relevance of services. These conditions are, in turn, influenced by the degree of access, awareness, availability, and attractiveness. In other words, digital dividends need to be built on analogue foundations, which makes core traditional development politics and projects central elements in bridging the digital divide.

To illustrate and contextualize the importance of this aspect, I draw on a few empirical case studies from countries in the Global South currently experiencing rapid digitalization.

The digitalization of Botswana has mushroomed: there have been substantial investments in digital infrastructure; the country scores high on Internet usage; Botswana has a national policy on Internet distribution and access points (including rural areas), and has among the highest percentages of Internet subscribers and social media users on the sub-Saharan mainland. Such statistics would indicate that Botswana has indeed become an Internet society – but if we look beyond these figures and focus on the actual impact of digitalization on everyday lives, a different picture emerges. Examining Botswana's two major industries – diamonds and cattle farming – the anthropologist Jo Helle-Valle[21] shows the relevance, or lack thereof, of digital technology and the Internet in the lives of ordinary people. The diamond industry is global and very much controlled by foreign capital – and it is through these connections that the industry is often seen as being fully digitalized. However, as Helle-Valle notes, "the Botswana work-force in this sector is typically manual labour, with little or no digital technological competence being required"[22]. In this major sector, Botswana is not very digitalized, nor is there perceived to be any great need for this.

Very different is the situation in Botswana's cattle industry. Helle-Valle shows how broad and innovative ICT projects have led to effective

18 | See for instance ITU, *Impact of broadband on the economy*, 2012, available at: https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf; op. cit. World Bank, 2016.

19 | Op. cit. Klimburg and Zylberberg, 2015; Dalberg Report, *Impact of the Internet in Africa: Establishing conditions for success and catalysing inclusive growth in Ghana, Kenya, Nigeria and Senegal*, 2013, available at: http://www.impactoftheinternet.com/pdf/Dalberg_Impact_of_Internet_Africa_Full_Report_April2013_vENG_Final.pdf

20 | Op. cit. Dalberg, 2013, p.9.

21 | Helle-Valle J., *What makes a society an internet society?*, 2015, available at: http://www.mediafrica.no/blog/2015/11/22/is-botswana-an-internet-society.

22 |Ibid, p.3.

management of the national stock and a thriving export industry. Thanks to new technology, most of the cattle in Botswana are now included in a system which, by means of a digital chip in each animal, can monitor and identify sickness, ownership, breed, theft, etc. Loaded into large databases, the data can be read through handheld devices such as smartphones, tablets or computers[23]. Through this system, cattle owners can communicate readily with veterinaries as well as buyers and sellers. The relevance of digital technology and access to the Internet depends on the set-up and the characteristics of different sectors.

Digital technology has also been used in Africa to strengthen internal solidarity and economic growth. In Kenya, fundraising campaigns through mobile phones and social media have raised considerable amounts of money for famine relief in the northeast of the country (Kenyans for Kenya campaign 2011). In 2007, the telecom company, Safricom, launched a mobile money service called M-PESA that attracted six million customers within two years, transferring billions annually. In 2008, M-PESA was launched in Tanzania[24], and has since expanded to Afghanistan, Albania, Egypt, India, Lesotho, Mozambique, Romania, and South Africa. Through M-PESA, people without bank accounts could leapfrog from traditional finance to digital economy[25]. Ushahidi, a digital app for rapidly reporting and tracking of outbreaks of violence in connection with elections, was launched in 2007; in the following year, Ushahidi became an international tech company based in Ngong Road, or what has become known as the Silicon Savannah, the tech-hub of East Africa. The social media were used to inform and coordinate help during the Westgate crisis in Nairobi, and to get blood donors following the attack[26]. A few years earlier, such mobilization would not have been possible.

Another country that has caught the digital wave is Rwanda. Considerable investments have been made in digital technology in schools as well as in infrastructure, aiming to "strengthen skills training centres and develop an ICT culture in schools as a means of creating a critical mass of IT professionals"[27]. Together with the Rwandan government, the Kigali Bus Service has invested in a cashless, card-based public transport ticketing system known as twende. By 2015, more than 30,000 customers had signed up. This initiative was part of the government's Smart Kigali programme for rapid modernization and digitalization of the capital[28].

While the digital dividends in these countries are evident, there are still many hurdles to be dealt with before the general populace can enjoy the extensive use of the Internet – with economy emerging as the main obstacle. The consumer costs are still too high for most people to be able to afford to use the social media and the Internet on a daily basis[29]. The bottom billion is taking only a modest share of the digital dividends:

23 | Op. cit. Helle-Valle, 2015, p.3.

24 | See infographic on Tanzania's mobile money revolution: http://www.cgap.org/data/infographic-tanzanias-mobile-money-revolution.

25 | Mbogo M., *The impact of mobile payments on the success and growth of micro-business: the case of M-Pesa in Kenya*, "Journal of Language, Technology & Entrepreneurship in Africa" 2010, 2(1), pp.182–203; Bright J. and Hruby A., *The rise of Silicon Savannah and Africa's tech movement*, Tech Crunch, available at: http://techcrunch.com/2015/07/23/the-rise-of-silicon-savannah-and-africas-tech-movement.

26 | Were D. K., *How Kenya turned to social media after mall attack*, CNN, 2013, available at: http://edition.cnn.com/2013/09/25/opinion/kenya-social-media-attack/ (accessed 25/02/16).

27 | Tafirenyika M., *Information technology super-charging Rwanda's economy*, "Africa Renewal" 2011, available at: http://www.un.org/africarenewal/magazine/april-2011/information-technology-super-charging-rwandas-economy.

28 | Dusabirane D., *East Africa: Airclerk's CEO envisions a cashless economy in Rwanda*, All Africa, 2015, available at: http://allafrica.com/stories/201511050868.html

29 | Op. cit. Global Commission on Internet Governance, 2016.

> *In the Central African Republic, one month of internet access costs more than 1.5 times the annual per capita income. Even mobile phones are expensive: the median mobile phone owner in Africa spends over 13% of her monthly income on phone calls and texting. And many poor lack the basic literacy and numeracy skills needed to use the internet*[30].

The digital gap is closely linked to the economic gap: the "haves" can make use of the new technology and reap digital dividends, while the "have-nots" are left behind. This is where development efforts can make a difference. By helping to bridge this infrastructural gap, donor countries can play a key role in contributing to the improvement of the technological business environment in the Global South[31].

1.2 Poor Network and Infrastructure – Urban-Centred Digitalization

The World Bank has developed a tool for measuring the degree of connectivity. To measure the availability, accessibility, and affordability of digital network and infrastructure, this infrastructure is divided into three miles: i) the first mile is the level where the Internet enters a country, ii) the middle mile is the level where the Internet spread through the country, and iii) the last mile is the level where the Internet actually reaches the end users. Additionally, the "invisible mile", which concerns important but less visible elements necessary for maintaining the integrity of these three levels, is often included in this division of infrastructure[32]. This tool is also useful for capturing characteristics and vulnerabilities pertaining to the cyber frontier. Much has been done in African countries to improve the first mile and the international gateway – the point where countries connect to the global Internet. Since 2009, thousands of kilometres of undersea broadband cables along the coasts of East Africa (see e.g. SEACOM) and West Africa (see e.g. WACS) have been bringing faster Internet to the continent, providing countries like Djibouti, Ghana, Ivory Coast, Kenya, Madagascar, Mozambique, Nigeria, Senegal, South Africa, Sudan, and Tanzania with high-speed services. While governments can negotiate higher Internet speed, better prices, and greater bandwidth, we should note that user conditions and Internet accessibility/availability depend on the middle mile, the national backbone, and intercity networks. These, in turn, depend on the degree of competition between public and private actors in the country. The rules of the market competition vary from one country to another, affecting the user side of digital networks and infrastructure. Liberalizing the market for the middle mile is an effective way of providing open access and the Internet to end users – but, as the World Bank has pointed out, this entails the risk "that the most popular routes – say, between the two main cities – are "superserved" while the rest of the country is underserved"[33]

.

In the Global South, the last mile is rarely served through fixed copper cables, as local access to networks is dominated by wireless alternatives. This is where the digitalization trajectory of the Global South differs most from the Global North, largely due to the differences between fixed and wireless networks. Whereas the Global North had achieved almost universal fixed-line access before wireless technology took over around 2001, most countries in the Global South never built fixed-line networks. The World Bank report sees this point as important because:

30 | Op. cit. World Bank, 2016, p.16.

31 | Various methodological models for fostering more efficient cyber-security capacity building have been developed; for an overview, see op. cit. Klimburg and Zylberberg, 2015, pp.20–26, and op. cit. Muller 2015.

32 | Op. cit. World Bank, 2016, p.205.

33 | Op. cit. World Bank, 2016, p.219.

> wireless networks [...] are not fully substitutable for fixed networks [...] either in usage (which rarely offers flat-rate pricing, without data limits) or in performance (where speeds are generally lower) [...] many developing countries are stuck with a second-class internet that may fail to deliver the expected benefits, especially for business users[34].

The 2016 World Bank report goes on to describe how countries in the Global South will have to struggle to achieve a fully sufficient middle mile, or a national backbone. Some countries may achieve such a backbone through private-public partnerships, but creating fixed-line networks in rural areas remains challenging and not very likely. Moreover, the report notes that fragile states, such as DR Congo and South Sudan, are unlikely to ever get fixed-line access, even in urban areas. Klimburg and Zylberberg mention the importance of Internet availability and adequate backbone network infrastructure, network ownership, and the geographic patterns of network development as essential for better business environments and improved digital dividends[35]. Furthermore, they hold that this situation creates "few incentives for local actors to either build network capacity in mostly rural areas or to expand network coverage. Development efforts need to focus on bridging this infrastructural gap, as a key determinant in an enabling business environment"[36]. The World Bank report finds the final mile is totally lacking in many countries – including Botswana, Burkina Faso, the Central African Republic, the Democratic Republic of Congo, Gabon, Kenya, Rwanda, Swaziland, Tanzania, and Togo[37]. In these countries, the analogue foundations for digital enterprises are weak, with no incentives for digital companies, such as online retailers. Unless global donor initiatives intervene, this situation points towards a trajectory of urban-centred digitalization in the Global South, with new kinds of societal vulnerabilities and a widening gap between the connected and the disconnected.

34 | Op. cit. World Bank, 2016, p.208.

35 | Op. cit. Klimburg and Zylberberg, 2015, p.9.

36 | Ibid.

37 | Op. cit. World Bank, 2016, p.255.

2. The Cyber Frontier and New Kinds of Societal Vulnerabilities

Individuals, businesses, and nations are depending more and more on data and digital systems. The Global South is following suit, rapidly expanding the cyber frontier. In this global transition into the digital era, it is easy to forget that the Internet was not invented for carrying the critical features and infrastructure that it does today, including key societal sectors like energy, power, economy, health, communications, and transport. The increasing interconnectedness of these features implies a major change in societal risk factors, highlighting the tight linkages between the domestic and international dimensions of politics. Global, complex, and rapidly shifting trends impinge on domestic political contexts, especially as regards the security dimension. Along with the opportunities and possibilities shaped by the digital revolution come new and more transnational challenges to the major areas of societal infrastructure as well as industry, innovation, and business. These threats cannot be reduced to technological concerns, as they are intertwined with international politics and global trends. Countries in the Global South with poor infrastructure and governance are rapidly being connected to the Internet – but the digitalization of these countries is often hollow. This can offer room for ill-intentioned cyberspace actors who may affect not only domestic problems in these countries, but global society as well.

Although the nations of the Global South are following in the path of the Global North and becoming more digitalized, they are taking a different route. For the Global North, digitalization has been a long-term sequential evolution: initially based on state-led investments

in fixed telephone infrastructure, it was followed by private initiatives and innovations, and then, building on this infrastructure established gradually over more than a hundred years, came the addition of mobile phones, smartphones, and the Internet. Countries in the Global South, by contrast, are leapfrogging straight into wireless technology, and mobile and Internet networks that are often built by the private sector (which obviates the need for investments in wiring with expensive copper cables). Jumping into the digital age has provided impoverished countries in the Global South with digital technology, new opportunities, and better connectedness. But the introduction of technology has often outpaced the establishment of state institutions, legal regulations, and other mechanisms that could manage new challenges arising from this technology. Digital technologies are being put to use before good, functional, and regulatory mechanisms have been developed and installed. The resultant shortcomings – in state mechanisms, institutions, coordination mechanisms, private mechanisms, general awareness, public knowledge, and skills – open the way to new kinds of vulnerabilities.

Countries in the Global South are weak in the know-how, awareness, institutions, and skills needed for dealing with cybersecurity issues. This vulnerability can be tackled through development assistance from donor countries to projects and activities focusing on awareness, knowledge, information, education, and employment[38]. In this context, digitalization and cybersecurity capacity building becomes integral to development assistance and the SDGs. Moreover, the dissemination of accurate information regarding security and structural aspects of the Internet is likely to make countries in the Global South more competent actors on the global arena where international cyber politics is developed, and thus better positioned to exert influence over their own position in the future.

3. The Security/Development Nexus

Combining cybersecurity with development assistance is in many ways contentious and likely to raise concerns about securitization of development assistance from the development community. Others claim that idea of connecting cybersecurity with development assistance may conversely contribute to de-securitizing it. Nevertheless, policymakers are increasingly recognising the building of cybersecurity capacity as a key component of development assistance. Some also highlight that this combination is particularly important because:

> *"the areas with the highest potential of economic growth correspond roughly with those where the security risks are the highest [and] the skills developed locally through cybersecurity trainings correspond to those needed to enable local businesses to scale up, without having to rely on outside, more expensive talent[39]."*

There are various models for cybersecurity capacity building, but they generally include three categories: technological, human, and organisational resources. Although helping to provide access to information and communication technology is seen as an important part of the development agenda[40], it is the building of institutional and human resources that should be the main priority of donor countries' development politics.

Botswana, Kenya, Mozambique, Myanmar, Rwanda, and Tanzania are experiencing rapid growth in digitalization and digital connectivity.

38 | See also Pawlak P., *Riding the digital wave – The impact of cyber capacity building on human development*, 2014, available at: http://www.iss.europa.eu/uploads/media/Report_21_Cyber.pdf (accessed 18/03/2016).

39 | Op. cit. Klimburg and Zylberberg, 2015, p.10.

40 | Op. cit. World Bank, 2016.

This connectivity fuels social, cultural, political, and economic (trans)formation, changing people's everyday lives. The up-side of this digital revolution is that it can help people out of poverty, and turn the economies in some countries of the Global South into some of the fastest growing in the world. When entrepreneurs, farmers, or fishermen can receive and transfer money digitally through the Internet, it becomes easier and safer to run small and medium-sized businesses. Connectivity also makes it possible to compare prices and different markets, which farmers, fishermen, as well as small and medium-sized businesses can put to good use. However, along with the upsides come some downsides, too. The digital trajectories of countries in the Global South often involve a different set of cyberthreats than those experienced elsewhere. Nir Kshetri has described the digitalization of the Global South as characterized by certain "hollowness"[41]. This "hollowness" may refer to weak institutions, poor organisational and individual defence mechanisms, better recruitment basis due to high unemployment and low wages, and a lack of capacity to manage risks and vulnerabilities in society[42]. Bot-herders[43] and other cyber-criminals tend to come from locations where high-paying IT jobs are rare or unavailable[44]; and in most countries in the Global South the growth of IT jobs is lower than the growth of Internet penetration[45].

The lack of capacity can stem from technological, behavioural, and policy-related factors. Generating innovation, driven primarily by commercial forces, without attention to security has left digital hollowness in these countries, which makes it easy to target unprotected devices and unskilled users, thus making these countries attractive to cybercriminals. Many countries in the Global South also lack the resources to build institutions to combat transnational crime[46]. Laws that recognise cybercrime, law enforcement mechanisms, personnel who understand cybercrime, as well as the awareness necessary for dealing with cybercrime – all these remain inadequate. Given their weak institutions, limited capacity, and generally low resources for fighting cybercrime, these countries are likely to remain attractive for cybercriminals also in the future.

Without sufficient attention to analogue foundations, this hollowness may escalate when countries in the Global South invest in more sophisticated ICT technology and digital connectivity. In addition to investments in security measures, such as anti-virus programmes, it is essential to improve basic knowledge about ICT. Poor and fragile institutions in many of these countries have contributed to this digital hollowness. Franz-Stefan Gady, a senior fellow at the EastWest Institute and a founding member of the Worldwide Cyber Security Initiative, has noted the statistics on the high numbers of PCs infected with viruses and malware in Africa and the reasons why these computers are easy targets for botnet operators[47]. Several experts have pointed out how rogue states and countries in the Global South become hosts to outlaw servers, also called "bulletproof hosting". The hosts of these servers operate beyond the reach of most

41 | Kshetri N., *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan, 2013, p.153.

42 | Kshertri N., *Diffusion and effects of cyber-crime in developing economies*, "Third World Quarterly" 2010, 31(7), p.1057.

43 | A botnet consists of many Internet-connected computers where components communicate and coordinate actions that can be used to send spam email of ddos (distributed denial-of-service) attacks. A bot herder or a botnet herder is a person who controls and maintains a botnet by installing malicious software in numerous machines, which can be controlled and used to attack or infect other machines.

44 | Sullivan B., *Who's behind criminal 'bot' networks?*, 2007 available at: http://www.unl.edu/eskridge/cyberbot3.htm.

45 | Op. cit. Kshetri, 2010, p. 1071.

46 | Cuellar M.-F., The mismatch between state power and state capacity in transnational law enforcement, "Berkeley Journal of International Law", 2004, 22(1), pp.15–58.

47 | Gady F.-S., *Africa's cyber WMD*, "Foreign Policy", 2010, available at: http://foreignpolicy.com/2010/03/24/africas-cyber-wmd/ (accessed 01/03/16).

law enforcers and enable cybercrime elsewhere[48]. Other authors have highlighted how certain vulnerabilities in the global network, as those in the SS7 (the network that allows cellular carriers to route calls, text, and other services to each other), which was built in the 1980s, can be used for surveillance by persons with illicit intentions, thus potentially undermining the privacy of cellular customers[49]. Through the SS7 "a single carrier in Congo or Kazakhstan [...] could be used to hack into cellular networks in the United States, Europe or anywhere else"[50].

Weak institutions and law enforcement mechanisms on cybercrime contribute further to the digital hollowness of countries in the Global South. Digitalization can be a key factor for economic and social development, and even democratization – but such development also opens new frontiers for criminals and others with bad intentions. As Hans Inge Langø has argued: "ICT can potentially be either a boon or a threat to democracy: it can aid peaceful opposition or violent rebellion; help governments enforce the rule of law or repress the population"[51]. Policymakers concerned with building cybersecurity capacity increasingly take such threats and risks into account when engaging in development assistance.

48 | Palmer M., *Rogue states play host to outlaw servers*, "Financial Times", 16 March 2016, available at: http://www.ft.com/intl/cms/s/2/c926b4ec-da25-11e5-98fd-06d75973fe09.html#axzz434Bv3Q84 (accessed 18/03/2016); Goncharov M., *Criminal hideouts for lease: Bulletproof hosting services*, Trend Micro Report, 2015, available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-criminal-hideouts-for-lease.pdf?_ga=1.24160381.61042644.1458131160 (accessed 18/03/2016).

49 | Landau S., *Surveillance or Security – The Risks Posed by New Wiretapping Technologies*, MIT Press, 2010.

50 | Timberg C., *German researchers discover a flaw that could let anyone listen to your cell calls*, Washington Post, 2014, available at: https://www.washingtonpost.com/ news/the-switch/wp/2014/12/18 /german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/ (accessed 18/03/2016).

51 | Langø H. I., *Cyber Security Capacity Building: Security and Freedom*, NUPI Report no. 1, 2016, Norwegian Institute of International Affairs, p.5.

The analogue foundations in a country usually determine the direction of its digitalization[52].

Cybersecurity plays a key role in ensuring sustainable economic and social development as well as achieving the international goals of combating poverty and inequality by 2030. Following from this, needs-assessments of cybersecurity maturity in the Global South will become a mapping activity increasingly applied in development assistance[53]. This includes the rule of law, education, and programmes to promote small and medium-sized businesses, as well as donor programmes facilitating the participation of recipient countries (civil society and governments) in the multi-stakeholder approach to Internet governance.

4. International Cyber Politics and Potential Swing States

The cyber frontier also influences the making of international politics. A country's position along the digital divide may often correspond to that country's cybersecurity, and presumably also to its cyber power. However, the particular trajectory of international cyber politics, including cybersecurity and strategies to negotiate it, can help to position the countries of the Global South as potent swing states in international politics. Inter-country exchange of information and experience is an important element in producing and developing new international cyber politics. Because of the rapid development of ICT, and the even more rapid pace of connectivity across the globe, old political challenges in international relations resurface in new and sometimes unexpected ways. In this political landscape, there is a dire

52 | See for instance Wagley R., *Telecom investments threaten privacy rights in Burma, US Campaign for Burma*, 2014, available at: https://uscampaignforburma.wordpress.com/2014/02/04/telecom-investments-threaten-privacy-rights-in-burma-2/ (accessed 01/03/16), and op. cit. Langø, 2016, pp.18–19.

53 | For an overview of different models measuring cyber capacity maturity in the Global South see op. cit. Muller, 2015, pp.7–10.

need for new international norms, policies, and trust. The multi-stakeholder approach, hailed as a way forward in international relations concerned with cyberspace, involves states, international organisations, private actors, think-tanks, and NGOs – but is still an immature or weakly defined institutional form[54].As a political topic in international relations, cyberspace incorporates new kinds of partnerships. There has been considerable research on international relations, global governance, and international organisation, but only a marginal part of this work has been focused on cyberspace and how it is changing well-established patterns in international relations. While international bodies like the UN, the EU, and NATO are important players in developing an international cyber policy, they are not able to fully incorporate the multi-stakeholder approach involving big private enterprises like Alibaba, Facebook, Google, or Huawei. On the other hand, as long as the technological revolution is run by the private sector, these actors have no formal say in international organisations like the UN[55]. While maintaining their focus and prioritized collaboration with international organisations (the UN, the EU, NATO, the AU, etc.), donor countries could also seek ways of working together with major private enterprises, perhaps especially in connection with development assistance and aid.

Another challenge is that many governments in the Global South lack the knowledge, awareness, and mature policies concerning cyberspace and cybersecurity necessary to participate fully in the global arena. In this context, there are potentials for donor countries and international organisations such as the EU to incorporate cyber capacity into their more traditional focus on development assistance concerned with institution building as well as cooperating with states, civil society, and NGOs, and developing partnerships of various kinds. Embarking on such programmes can contribute to new partnerships and sustainable development with social and economic growth, as well as giving donor countries and organisations such as the EU an advantage in the global arena of an international cyber policy. With current international politics on cybersecurity and Internet governance, the potential of recipient countries as swing states in international politics increases.

Conclusions

This article has drawn on the cyber frontier perspective in order to explain certain features of the current international politics pertaining to security and development assistance. New kinds of societal vulnerabilities emerge and new power relations are being forged. With its emphasis on (trans)formation and continuity, the analysis clarifies the connections between digitalization, economic growth, and cybersecurity. This triple knot pointed at a tendency where the "haves" can reap the digital dividends, while the "have-nots" are being left behind. In this way increased Internet access entails a need for greater development assistance and engagement. Bridging the digital divide also requires analogue foundations, knowledge, awareness, and a digital environment where the focus on cybersecurity will be increasingly important.

There are opportunities for donors such as the EU in this field. Digitalization brings with it a pressing need for knowledge, education, institution building, and experience-sharing among countries and regions. Although traditional development mechanisms can be applied to enhance sustainable development and cybersecurity capacity, this combination also introduces new aspects and dilemmas. This trajectory of digitalization in the Global South has produced a set-up in which

54 | Raymond M. and L. Denardis, *Multistakeholderism: anatomy of an inchoate global institution*, "International Theory" 2015, 7(3), pp.572–616.
55 | The multi-stakeholder process seems to be gaining a footing also in international bodies like the UN. Although most of those speaking at the December 2015 WSIS+10 meeting at the UN General Assembly were state representatives, spokespersons from several private companies also took the floor.

private actors have assumed a dominant role. For donors, this represents a challenge, because many of the structural assumptions about ownership, authority, and governance that have underpinned traditional development policies are now turned upside-down.

Distinct properties of cyberspace – such as the fact that it has no borders, has few rules, and the free flow of information – trigger new kinds of challenges with regard to international politics, security politics, sustainable development, and the implementation of the SDGs. This examination of the frontier peculiar to cyberspace has highlighted the technological, organisational, and human dimensions as well as the local, national, regional and international levels of digitalization. Building capacity in cybersecurity represents a relatively new political field (not properly included in the UN's SDGs or even in the World Bank's 2016 World Development Report) where donors like the EU may continue their long-term foreign policy traditions by incorporating a new policy field. ■

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. Feldmana 4/9-10, 31-130 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 ADRESSED TO

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

FROM THE FOLLOWING SECTORS

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

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

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

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

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY JOURNAL