VOLUME 3 (2017) ▪ ISSUE 2

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 3 (2017), Issue 2, 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

In the past few months, we have witnessed a number of critical events, all of them of pivotal importance from the cybersecurity point of view. They are different in nature and cause diverse consequences. This issue of the European Cybersecurity Journal provides a thorough analysis of selected critical challenges.

In recent times, the discussion on artificial intelligence has flourished. Not only do market leaders discuss and develop new directions of actions, but the topic has also reached the top of the political agenda. For instance, in February, the European Parliament adopted a resolution to regulate the development of artificial intelligence and robotics. In his text, Guido Noto La Diega argues that while the discussion about the future of AI and robotics is getting mature, we still lack in-depth debate on the security of these systems. There is no doubt that the future belongs to these new technologies, and the argument that security needs to be the foundation for its development seems to be truly valid.

Around three months ago, the WannaCry ransomware attack spread around the world, impacting systems in around 150 countries. This unprecedented cyberattack once again proved that in terms of cyberspace both prevention and quick response are crucial. In her article, Aneta Urban takes a slightly different perspective when analysing the attack. She looks at communication strategies performed by both the international and Polish institutions during the attack. Some interesting conclusions from the text may be used as lessons learnt for the future.

A few weeks ago, another phase of the development of cyber norms by the UN GGE ended in deadlock. This brings forth plenty of questions on the future of building a global stability regime for cybersecurity. The article written by Robert Morgus elaborates on another process also important from the point of view of cyberspace stability. He presents an analysis of the Wassenaar Arrangement multilateral regime, aimed at controlling the proliferation of intrusion software, and points out some scenarios for the future.

The current issue of the European Cybersecurity Journal touches also upon other matters, not related to particular events, but universal and equally important. By reading the text prepared by Wiesław Goździewicz you will learn about various aspects of private-public cooperation in the military area. In her article, Giulia Pastorella proves the importance of endpoint devices security – a problem often neglected and underestimated. The interview with Szymon Kowalczyk from Tauron, one of the largest energy holding companies in Central Europe, sheds light on the cybersecurity of critical infrastructure. Last but not least, the article written by Adam Palmer provides an account of NATO's response to cyberattacks.

Finally, I would like to use this opportunity to invite you to the 3rd edition of the European Cybersecurity Forum that will take place on 9th–10th October 2017. During the event, several topics discussed in this issue will be developed even to a greater extent.

CONTENTS

CYBERSEC
EUROPEAN
CYBERSECURITY FORUM

Krakow
9-10.
10.
2017

3rd European Cybersecurity Forum

Dealing with cyber disruption

#CSEU17 | www.cybersecforum.eu

ANALYSIS

THE EUROPEAN STRATEGY ON ROBOTICS AND ARTIFICIAL INTELLIGENCE: TOO MUCH ETHICS, TOO LITTLE SECURITY

DR GUIDO NOTO LA DIEGA
Dr Guido Noto La Diega is a Lecturer in Law at the Northumbria University and President of "Ital-IoT", the first Centre of Multidisciplinary Research on the Internet of Things. Fellow of the Nexa Center for Internet and Society, he completed a PhD in Intellectual Property and a Postdoc in Cloud Computing Law at Queen Mary University of London. His expertise in cyber law was recently recognised by the EU Court of Justice's Advocate General in the Uber case. Over nearly a decade of academic career in Italy, Germany, Switzerland, and the United Kingdom, Dr Noto La Diega has published extensively in peer-reviewed journals and presented his research in several national and international conferences and symposia. Dr Noto La Diega provides consultancy in matters of ethics by design, privacy, consumer protection, and intellectual property.

There is an increasing interest in the ethical design of robots. As evidence of this fact, one may refer to some recent reports[1] and the European Parliament's resolution on "civil law rules on robotics"[2].The latter will be the primary focus of this analysis since the EU Parliament "is the first legal institution in the world to have initiated work of a law on robots and artificial intelligence"[3], but the former also deserves a mention.

In June 2016, the European Parliament's Science and Technology Options Assessment Panel published a report on the ethical aspects of cyber-physical systems (CPS). The research was conducted by the Technopolis Group and managed by the Directorate-General for Parliamentary Research Services' Scientific Foresight Unit. CPS are "smart systems that include engineered interacting networks of physical and computational components"[4]. Given this definition, most of robots currently deployed qualify as CPS; therefore the rules about the latter apply also to the former. The main concerns expressed in the report regarded unemployment, excessive delegation of tasks, safety, responsibility, liability, privacy, and "social relations". The last issue gives rise to

1 | Science and Technology Options Assessment Panel, "Scientific Foresight study: Ethical Aspects of Cyber-Physical Systems", June 2016; Directorate-General for Internal Policies - Policy Department for Citizens' Rights and Constitutional Affairs, "European Civil Law Rules in Robotics", Study for the JURI Committee, 2016.

2 | European Parliament, Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), 2017.

3 | Trojnarski, M., „The Future Is Now - The Law on Robots, published in February 2017, (online) www.lexology.com/library/detail.aspx-?g=3e9ffdfb-8a47-42c1-9284-c5ac12ff83c4.

4 | Setiawan, A. B., Syamsudin A., Sastrosubroto A. S., "Information security governance on national cyber physical systems", [in] International Conference on Information Technology Systems and Innovation (ICITSI), 2016.

a fundamental question whether robots should "acquire some form of moral sense"[5]. The proposed solution is more focused on regulation rather than on "ethics by design". It is submitted, indeed, that "regulations need to be updated to ensure that individuals are not harmed and that the desired benefits outweigh the potential unintended consequences"[6]. However, the report claims that "a governing or guiding framework for the design, production and use of robots is needed"[7].

Four months later, the European Parliament published a commissioned report on the civil law rules applicable to robotics[8]. A significant part of the report was dedicated to the development of ethical principles in robotics. The main principles concerned the protection from physical harm, the right to refuse to be cared for by a robot, human liberty, privacy, data protection, protection against manipulation and dissolution of social ties, equal access to advances in robotics, and restrictions imposed on enhancement technologies (against the transhumanist and posthumanist philosophies). The report approves of the Charter of Robotics proposed by the European Parliament's Committee on Legal Affairs (JURI)[9], which is seen as a tool to ensure that ethical principles govern robotics in "harmony with Europe's humanist values"[10]. In commenting on the JURI's draft report on robotics[11] and its proposal of a new legislative instrument, the report affirms that "many legal sectors are coping well with the current and impending emergence of autonomous robots since only a few adjustments are needed on a case-by-case basis"[12]. Conversely, it is suggested that tort law should be rethought. Although the report approves of the idea to adopt an instrument for a 10-15-year period, it also recognises that it could soon become obsolete, especially because of the convergence between nanotechnology, biotechnology, information technology, and cognitive science.

The motion has its roots in a report drafted by an ad hoc working group set up in 2015 by the JURI[13]. It included a motion for a European Parliament resolution and an annex with detailed recommendations to the Commission as to the content of a legislative proposal.

In February 2017, the European Parliament adopted the resolution with "recommendations to the Commission on Civil Law Rules on Robotics"[14]. Even though the focus should have been on the civil law rules, ethics played a key role. One need only mention that the resolution refers to words "ethics/ethical" as many as 50 times, thus making them some of the most recurring terms, following "robot/robotics", "human", "whereas", and "develop" (with "liable/liability" occurring only 39 times), based on our calculations.

> "The most controversial point regards the status of robots as electronic persons.

The resolution aims at the introduction of EU rules to unleash robotics' and AI's potential, while guaranteeing a high level of safety and security. Prima facie, liability and security should be at the core of the resolution, but we sadly observe that ethics seem to play a dominant role.

The rationale behind this is largely driven by fear. Indeed, according to the rapporteur Mady Delvaux, a robust EU legal framework should be created (as if no applicable law already existed, which is not the case), in order to "ensure that robots are and will remain in the service of

5 | Op. cit. Science and Technology Options Assessment Panel, 2016, p.8.
6 | Ibid.
7 | Ibid p.36.
8 | Op. cited Directorate-General for Internal Policies, 2016.
9 | European Parliament, Draft Report of 31 May 2016 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)), 2016, (online) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN.
10 | Op. cit. Directorate-General for Internal Policies, 2016, p.5.
11 | Op. cit. European Parliament, 2016.
12 | Op. cit. Directorate-General for Internal Policies, 2016, p.6. An example of this is the copyright of robot-generated works (see Noto La Diega, 2016).
13 | Op. cit. European Parliament, 2016.
14 | Op. cit. European Parliament, 2017.

humans[15]. In the perennial battle between singularitarians and AItheists[16], the European Parliament can be ascribed to the former fringe. Singularitarians believe that superintelligence is "the most important and most daunting challenge humanity has ever faced"[17], and that in six years "the human era will be ended"[18]. The author joins Searle in believing that these apocalyptic scenarios are implausible, since they require maliciously motivated machines willing to destroy us all. However, this would involve consciousness, which is what robots do not have[19].

Certainly, the most controversial point regards the status of robots as electronic persons. Indeed, the Commission is called on to consider the implications of the creation of a specific legal status for robots in the long run, "so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently"[20]. Even though the suggestion may seem extreme, it may prove to be successful, for at least three reasons. First, robots are becoming more and more similar to humans (anthropomorfisation and AI). Second, humans are becoming increasingly akin to robots (artificial enhancement). Third, the robot's legal personality would be profitable for the robotic industry. Indeed, the reason why we demand from robots a higher level of security and accuracy, as compared to human standards, is that there is still a fundamental difference between robots and humans. The former cannot go to prison, and the purpose of the law (especially of criminal law) is to keep peace in society by finding someone to blame and punish for a number of behaviours which are viewed as unacceptable. Electronic personality could be the prerequisite of the social acceptance of robots as potentially liable, and this could enable an unprecedented market penetration.

> "The European strategy regarding robots is threefold, with ethics playing an eminent role. The principles which the Parliament asks to take into consideration to reduce the risks are human safety, health and security, freedom, privacy, integrity, dignity, self-determination, non-discrimination, and data protection.

The European strategy regarding robots is threefold, with ethics playing an eminent role. The principles which the Parliament asks to take into consideration to reduce the risks are human safety, health and security, freedom, privacy, integrity, dignity, self-determination, non-discrimination, and data protection. One can easily see that it is not always possible to pursue these objectives at the same time. An action that maximises human safety could undermine self-determination. Minimising security threats could mean jeopardising privacy. Striking a balance between opposite principles is an inherently human operation (and one which is required constantly to interpret and apply the law).

Firstly, there is the "Charter of Robotics" that would regulate who would be held accountable for the social,

15 | European Parliament, Press Release: "Robots: Legal Affairs Committee calls for EU-wide rules", published on 12 January 2017, 2017(b).
16 | Floridi, L., "Should we be afraid of AI?", essay published on www.aeon.co, 2016, (online) https://aeon.co/essays/true-ai-is-both-logically-possible-and-utterly-implausible.
17 | Bostrom, N., "Superintelligence: Paths, Dangers, Strategies", Oxford University Press, 2014.
18 | Vinge, V., "What is The Singularity?", article written for the VISION-21 Symposium sponsored by NASA Lewis Research Center and the Ohio Aerospace Institute, March 30-31, 1993, p.11, (online) http://edoras.sdsu.edu/~vinge/misc/singularity.html.
19 | Searle, J. R., "What Your Computer Can't Know", essay and book review, [in] The New York Times Book Review, 2014, (online) http://static.trogu.com/documents/articles/palgrave/references/searle%20What%20 Your%20Computer%20Can%E2%80%99t%20Know%20by%20John%20R.%20Searle%20%7C%20The%20New%20York%20Review%20of%20Books.pdf.
20 | Op. cit. European Parliament, 2017, paragraph 59.f.

environmental and human health impacts of robots (e.g. kill switch). The charter comprises three documents: a code of conduct for robotics engineers, a code for research ethics committees when reviewing robotics protocols and model licences for designers and users. The charter aims to be "a clear, strict and efficient guiding ethical framework for the development, design, production, use and modification of robots"[21]. According to the European Parliament's resolution on robotics, the existing EU legal framework should be "updated and complemented, where appropriate, by guiding ethical principles"[22]. It is obvious, however, that the law cannot be updated by some ethical guidelines; indeed, law and ethics belong to discrete realms.

As to the ethical content of the charter, the EU resolution on robotics clearly mirrors the current worries about algorithmic accountability and the so-called black box. Indeed, the first ethical principle to consider is transparency. The said principle means that "it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have a substantive impact on one or more persons' lives"[23]. This is already covered by the rules on automated decision-making under the Data Protection Directive, as strengthened by the General Data Protection Regulation that will come into force in May 2018. Therefore, the guideline on this point seems redundant. However, the specification whereby "robots should be equipped with a 'black box' which records data on every transaction carried out by the machine, including the logic that contributed to its decisions"[24] could be of some use. It must be said, nonetheless, that one of the main problems of some AI technologies (e.g. deep learning) is that the machines inform you about the result, but not about the relevant reasons. Therefore, algorithmic accountability risks being just a chimera.

Another "ethical" principle dealt is privacy. According to the resolution, "special attention should be paid to robots that represent a significant threat to confidentiality owing to their placement in traditionally protected and private spheres and because they are able to extract and send personal and sensitive data"[25]. Firstly, one should notice that the reference to confidentiality is incorrect. From the context, it would seem that the document does not refer to trade secrets (also known as confidential information), but to privacy. Secondly, it would seem that the point is rather futile, if one considers that data protection by design and by default approaches are mandatory under the General Data Protection Regulation.

In addition to transparency, it is submitted that the ethical framework should be based on several principles: beneficence, non-maleficence, autonomy and justice, as well as the principles and values enshrined in Article 2 of the Treaty on the EU and in the Charter of Fundamental Rights of the EU, such as human dignity, equality, justice and equity, non-discrimination, informed consent, private and family life, and data protection. The potpourri is completed by the reference to the "other underlying principles and values of the Union law, such as non-stigmatisation, transparency, autonomy, individual responsibility and social responsibility, and on existing ethical practices and codes"[26]. One could wonder why some of the principles that were indicated as paramount[27], such as safety and security, are not openly referred to here. However, the most important note is that what already has been said about the impossibility to embed so many competing values in the design, and striking a balance as an inherently human operation applies all the more here.

The Policy Department for Citizens' Rights and Constitutional Affairs[28] criticises the call for the charter. Firstly, unlike most codes of conduct, which originate from the relevant industry itself (self-regulation), the charter is proposed by the Parliament, as opposed to the industry. Secondly, lacking legal status[29], charters, codes, guidelines, etc. are merely "tools used to

21 | Ibid. paragraph 11, italics added.
22 | Ibid.
23 | Ibid. paragraph 12.
24 | Ibid.
25 | Ibid. paragraph 14.
26 | Ibid. paragraph 13.
27 | Ibid. paragraph 10.
28 | Op. cit. Directorate-General for Internal Policies, 2016.
29 | Cour de Cassation, chambre commerciale, 29 June 1993, No 91-21962, Bull. civ. 1993, IV, 274, 194.

communicate with clients, civil society or a company's employees"[30]. In particular, the enforceability against third parties seems to be excluded, unless the terms are included in a contract (e.g. of robot purchase).

The second leg of the strategy is the obligatory insurance scheme. Recognising the complexity of allocating responsibility for damage caused by increasingly autonomous robots, the European Parliament recommends obligatory insurance, along the lines of the vehicle insurance. However, the robot insurance should not only cover human acts, but it "should take into account all potential responsibilities in the chain"[31].

Thirdly, the establishment of the European agency for robotics and artificial intelligence is meant to supply public authorities with technical, ethical and regulatory expertise. The agency will manage a system of registration for robots for the purposes of traceability and the implementation of further recommendations.

It is interesting that, having placed so much emphasis on designing "ethical" robots, the resolution calls on the Commission and the Member States to support ethics by design only once, cursorily, in the section dedicated to "Intellectual property rights and the flow of data" (which is actually focused on privacy). Again, it provides evidence of a clear value hierarchy, where ethics comes before security.

The EU safety and security strategy looks way less developed than the one regarding ethics. It deals with two issues: standardisation and real-life scenarios testing. The resolution calls on the Commission to work on the international harmonisation of technical standards mainly to ensure interoperability, but also to guarantee a high level of product safety and consumer protection (e.g. ISO/TC 299 Robotics). Again, the Parliament does not seem to be aware that there is a balance to strike, a trade-off between interoperability and safety. As for the second part of the EU robotics security strategy, the Parliament observes that testing robots in real-life scenarios is essential for risk assessment and technological development. The Member States should identify areas where experiments with robots are permitted, in compliance with the precautionary principle. This is already being done, especially with regards to drones, but the suggestion must meet a wider positive reception.

Finally, in May 2017, the public consultations on the "Future of Robotics and Artificial Intelligence" were concluded. We shall see whether, as alleged in the accompanying text, the results "will help the European Parliament to define potential next steps and future policies at EU level"[32]. Reading one of the few submissions already available, one can see why ethics is becoming increasingly important. European Digital Rights (EDRI) point out that in order to encourage innovation and global competitiveness, the EU should take action to improve ethical standards because "customers buy products that respect their values"[33]. Privacy by design and default are an essential way to create and maintain trust. Products that are not privacy friendly, or that are found to have privacy issues, will suddenly become less attractive for customers.

In conclusion, the European strategy on robotics seems affected by two main problems: an excessive emphasis on ethics at the expense of security, and more generally, a lack of awareness of the critical role played by the operation of striking a balance between competing interests. Balancing is pivotal to the interpretation and application of the law. And the current development of AI technologies does not enable the delegation of the operation to robots. ■

30 | Op. cit. Directorate-General for Internal Policies, 2016, p.26. For a minor exception, see the French professional associations' codes of conduct.

31 | Op. cit. European Parliament, 2017, paragraph 57.

32 | www.europarl.europa.eu/committees/en/juri/public-consultation-robotics-introduction.html.

33 | EDRI, "EDRi's response to the European Parliament's consultation on Civil Law Rules On Robotics", published on 24 April 2017, (online) https://edri.org/files/consultations/civillawrulesonrobotics_edriresponse_20170424.pdf.

ANALYSIS

COMMUNICATION ON CYBERSECURITY ISSUES BY INTERNATIONAL AND POLISH INSTITUTIONS: THE CASE OF THE WANNACRY RANSOMWARE ATTACK

ANETA URBAN
Senior Project Coordinator at the Kosciuszko Institute. Graduate in American Studies from the Jagiellonian University and a student of Political Science, Aneta takes great interest in advertising, marketing, the use of new media in political marketing as well photography and visual arts. At the Institute, she is in charge of establishing partnerships with public administration and non-governmental institutions as well as coordinating the execution of creative concepts underpinning the Institute's projects.

"The Largest ransomware attack in internet history", "the biggest ransomware offensive in history", "the WannaCry attack is a wake-up call" – the headlines of the various international media have flooded the internet, warning about the ransomware attack, which has massively spread around the world since 12 May 2017. It is known as WannaCry, WannaCrypt, WanaCrypt0r, WRrypt, and WCRY.

WannaCry is ransomware that contains a worm component. It attempts to exploit vulnerabilities in the Windows SMBv1 server to remotely compromise systems, encrypt files, and spread to other hosts[1].

According to US-CERT and numerous open-source reports, the campaign has affected various organisations in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages[2].

1 | WHAT IS WANNACRY/WANACRYPT0R?, National Cybersecurity and Communications Integration Center, [in:] US-CERT, United States Computer Emergency Readiness Team, [online] https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware_S508C.pdf.

2 | Alert (TA17-132A), Indicators Associated With WannaCry Ransomware, [in:] US-CERT, United States Computer Emergency Readiness Team, [online] https://www.us-cert.gov/ncas/alerts/TA17-132A.

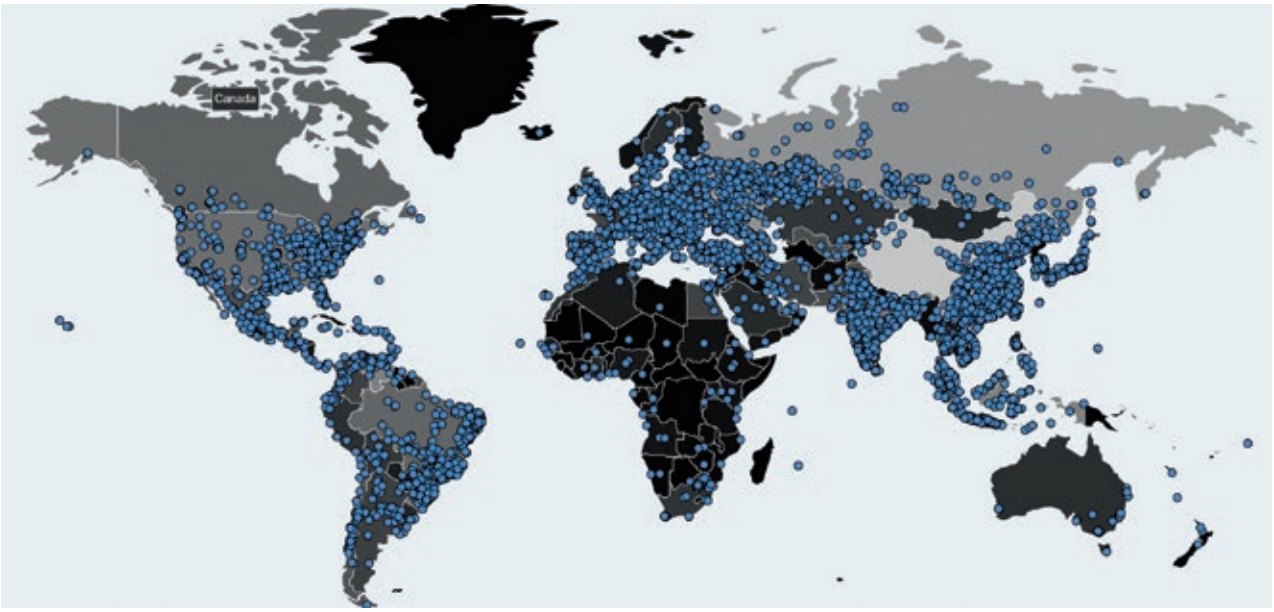


Figure 1. Infection Map (age: 0h 57m 59s). Source: Malwaretech.com[3].

Cybersecurity, being the main challenge of today's fast-developing world, has not yet become the main subject of interest of the average citizen. However, the landscape of building cybersecurity awareness is changing constantly – there are plenty of programmes, aimed at complementary education of connected web users and strengthening readiness within companies.

According to the Eurostat's *Digital economy & society in the EU* report, 71% of the interviewees admitted to providing some kind of personal information online, including 40%, who have also provided payment details[4]. It is obvious that without proper education about the threats and risks and also without the necessary tools securing a person's actions in the internet, it is not a big challenge for the hacker to take over not only the personal data, but also to access their banking information. The survey shows, that only almost 2 out of 10 EU interviewees use anti-tracking software, which can prove low cybersecurity awareness among the internet users.

One of the basic roles of public institutions and the media is to share the information about threats to citizens' security, but also inform about the potential risks. In today's world, cybersecurity is not being taken seriously by all the mainstream media yet, but it is gaining attention incrementally. Therefore, when the WannaCry ransomware attack occurred, the institutions and media had taken various measures to inform about the possible threat and provide help to prevent unwanted consequences.

Reaction and recommendations of the international institutions

1) ENISA's response

The European Union Agency for Network and Information Security (ENISA) has shared its first publication on WannaCry ransomware three days after the attack, publishing the *WannaCry Ransomware Outburst* information note. Before the publication of the note, ENISA also had used the Twitter account to promote their report *Cyber security and resilience for Smart Hospitals*, using the connection between the subject of the report and the big numbers of hospitals and healthcare facilities affected as a result of the attack. In the document about the WannaCry ransomware itself, ENISA defined

3 | MALWAREINT map, [online] https://intel.malwaretech.com/botnet/wcrypt/?t=24h&bid=all.

4 | Digital Economy & Society In The EU. A Browse Through Our Online World In Figures, 2017 edition, [in:] Eurostat, [online] http://ec.europa.eu/eurostat/cache/infographs/ict/index.html.

Figure 2. Timeline of events. Source: ENISA's WannaCry Ransomware Outburst[7].

the attack and named it as *one of the top threats identified in ENISA Threat Landscape report 2016*[5]. The background and the infection process have been explained very understandably for the average reader. At the end of the report, ENISA shares recommendations for the users at risk of being hit by WannaCry and advice on protecting their files in anticipation of upcoming possible threats. Then, the authors of the information note warn about the necessity of being prepared for this kind of incident, such as self-propagating ransomware, which has been identified by ENISA as the next big threat to cybersecurity. On 15 May, the Agency also published a press release, confirming the cooperation of ENISA and several European Member States in order to *assess the situation caused by the WannaCry Ransomware at European level (...) Udo HELMBRECHT, Executive Director of ENISA, said "as the European Cybersecurity Agency, we are closely monitoring the situation and working around the clock with our stakeholders to ensure the security of European citizens and businesses, and the stability of the Digital Single Market. We are reporting on the evolution of the attacks to the European Commission and liaising with our partners in the European Union CSIRT Network"*[6].

5 | WannaCry Ransomware Outburst,[online] https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst.

2) Europol's response

The European Union Agency for Law Enforcement Cooperation (Europol) reacted to the information on the WannaCry attack two days earlier than ENISA and published a tweet: *Europol's @EC3Europol is supporting countries. #WannaCry #Ransomware attack at unprecedented level and requires international investigation*[8]. In the news article published by Europol on the same day the users were assured of ongoing investigation and encouraged to learn about the resources on cybercrime and ransomware and protect the data and users' devices[9]. Europol continued to share information about the issue of ransomware on Twitter, by publishing infographics and threat maps, explaining the risks and building awareness among the followers. Also, on the Twitter profile

6 | WannaCry Ransomware: First ever case of cyber cooperation at EU level, [online] https://www.enisa.europa.eu/news/enisa-news/wanna-cry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level.

7 | WannaCry Ransomware: First ever case of cyber cooperation at EU level, [online] https://www.enisa.europa.eu/news/enisa-news/wanna-cry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level.

8 | Europol's Twitter status, [online] https://twitter.com/EC3Europol/status/863350056719699969.

9 | Wannacry Ransomware: Recent Cyber-Attack, [in:] Europol's newsroom, [online] https://www.europol.europa.eu/newsroom/news/wannacry-ransomware-recent-cyber-attack.

of the Europol's European Cybercrime Centre (EC3), the information on the ransomware has been spread since the 13 May – EC3 has shared the recommendations and solutions of the various institutions, such as Spanish El Centro Criptológico Nacional[10] or UK's National Cyber Security Centre[11]. International cooperation in this field appeared to be extremely vivid, assuring the internet users of the joined forces of worldwide institutions to protect the data and privacy of the citizens.

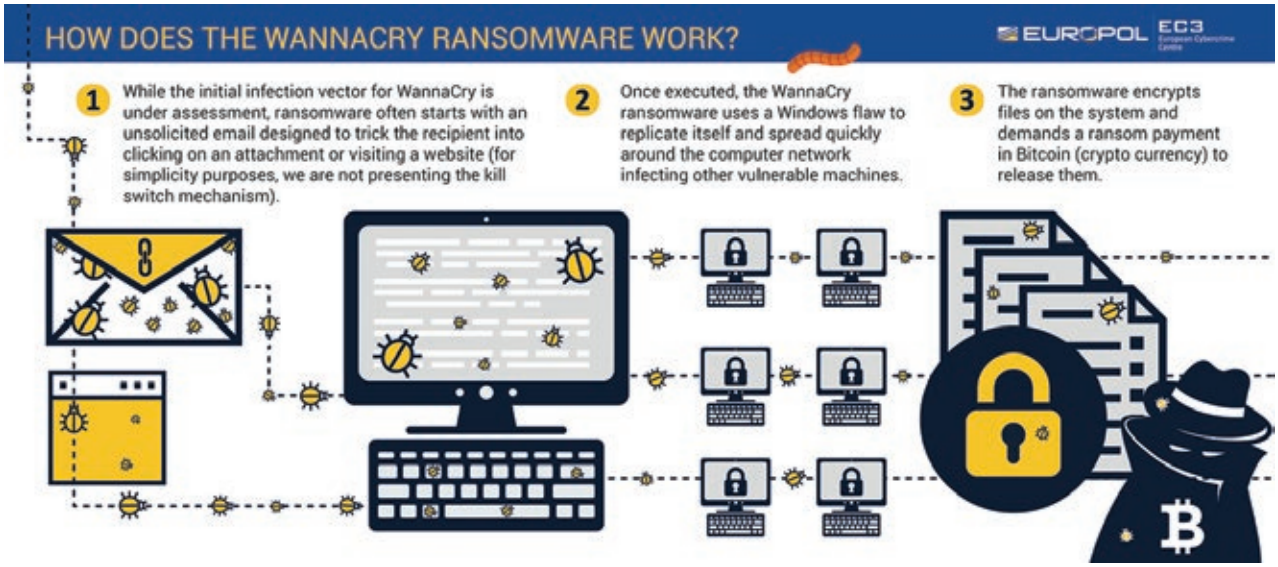
A week after the attack, Europol shared a document similar to ENISA's information note. Providing easy-to-understand infographics, the authors explained the nature of the attack, the ways of spreading the ransomware, recommendations for the potential victims and instructions how not to become one. The publication is very comprehensible and provides basic, concise information for the interested reader.

Figure 3. How does the wannacry ransomware work? Source: Europol[12].

Reaction and recommendations of the Polish institutions

Since the beginning of the WannaCry campaign, international institutions have been effective in their work on sharing information about the attack and "teaching" the users how to save themselves from further consequences. The institutions responsible for cybersecurity in Poland also informed public opinion about the attack in various ways. On 13 May, the spokesperson of the Internal Security Agency informed that the Agency and the institutions under the Ministry of Digital Affairs did not identify Poland as a target of the attacks[13].

Afterwards, according to the Polish portal dedicated to cybersecurity – *Zaufana Trzecia Strona*[14], the message was allegedly sent on 14 May to selected institutions by the Governmental Computer Emergency Response Team, responsible for coordination of emergency responses within the government administration sector. CERT.GOV.PL operates within the structures of the Internal Security Agency. The message included the warning and technical information, which could be



10 | EC3's Twitter status, [online] https://twitter.com/EC3Europol/status/863492271911645184.
11 | EC3's Twitter status, [online] https://twitter.com/EC3Europol/status/863698000878678016.
12 | How Does The Wannacry Ransomware Work? [in:] Europol's WANNACRY RANSOMWARE, [online] https://www.europol.europa.eu/wannacry-ransomware.
13 | Globalny atak hakerski ominął Polskę? Jest komentarz rządu, [online] http://kurier.pap.pl/depesza/174393/Duzy-atak-hakerski-ominal-Polske--Jest-komentarz-rzadu.
14 | Komunikacja polskich instytucji państwowych na temat WannaCry – analiza, [in:] Zaufana Trzecia Strona, [online] https://zaufanatrzeci-astrona.pl/post/komunikacja-polskich-instytucji-panstwowych-na-tem-at-wannacry-analiza.

helpful in passing necessary information about the threat campaign, instructions about preventing further infection and encouragement to share information about the next possible incidents with the proper security services. However, the author of the *Zaufana Trzecia Strona* article has identified some major mistakes in the ways of communication about the threat, which had caused the information chaos.

On Monday, an article was published by the CERT Polska team which operates within the structures of NASK (Research and Academic Computer Network). The article was similar to the releases by the ENISA and Europol. The publication aimed to explain the threat briefly and addressed some of the institutions and companies affected by the ransomware. The article not only included explanations of the infection process, its sources and impact, but also a lot of technical information about the ransomware for professionals interested in the way in which it functions. Previous information provided by the Internal Security Agency about the non-infected Polish devices was denied by CERT, which has indicated over 1,000, and subsequent 4,000 infections of the Polish IP addresses. According to *Zaufana Trzecia Strona*, on the profile of the Polish National Cyber Security Centre, a tweet was published identifying only 174 IP addresses – something completely different from the data published by the Polish CERT. It is said that the tweet was deleted after one hour from publication[15].

The CERT did not prepare any infographics for the readers, helping to understand the threat better, but it has demonstrated the resources by a foreign company. At the end of the publication, the author shares some brief advice for the infected users and ways to avoid the risk.

Conclusions

The communication of international institutions, such as ENISA and Europol, can prove years of experience in fighting similar threats and preparing the strategy of communication and crisis management. These authorities can be a role model as regards the ways of communicating issues that may be technically complicated and difficult to understand for the average internet user. However, it is crucial to inform public opinion in a comprehensible manner, using visual content and graphics. It can be very helpful for the readers to gather information easily so that they may protect themselves in the best way possible. The international institutions discussed in this article proved their experience and preparation for such incidents.

As regards the Polish institutions, one of the advantages of their actions can be their rapid response to the threat and immediate action taken. However, according to the author of the *Zaufana Trzecia Strona* analysis, the most accurate source of information about the incident were not the institutions' websites, but Twitter discussions among private users and the independent experts' opinion.

The WannaCry attack was broadly covered by the international media such as *The Telegraph*, *Forbes*, *Wired*, *The Verge*, *The Guardian* and many more. In the Polish media, the issue was precisely covered, but mainly by titles specialised in the issue of security, such as Niebezpiecznik, Sekurak, and previously mentioned *Zaufana Trzecia Strona or Chip.pl*. The mainstream media only mentioned the threat, but did not place headlines on their front pages. This may prove still low awareness of Polish public opinion concerning this kind of threats and low interest in the issue of cybersecurity.

Poland does not have a long history of facing critical situations in cybersecurity and handling the urgent need of brief communication with public opinion. We are still learning and developing the solutions that can be crucial in fighting and responding to potential threats. Communication in situations like the WannaCry attack, like every unexpected incident, has its own demands. Therefore, we should gather best practices from abroad and implement them in the Polish reality. ■

15 | Ibid.

ANALYSIS

CONSTRAINING THE SPREAD OF MALICIOUS CYBER CAPABILITY POST-WASSENAAR INTRODUCTION

ROBERT MORGUS
is a policy analyst with New America's Cybersecurity Initiative, where he researches and writes at the intersection of cybersecurity and international affairs. His current work focuses on international capacity building, international norms development, and cyber risk and insurance. In the past he has authored reports on sanctions and export controls, internet freedom, and internet governance. His work has been showcased in the New York Times, TIME, Slate, and others. He serves as a research advisor for the Global Commission on Internet Governance and the Global Commission on the Stability of Cyberspace.

Introduction

In late November 1953, between rounds of golf at Bermuda's Mid Ocean Club, Dwight D. Eisenhower pored over a speech he had written days earlier with the American public as the intended audience. His goal was to modify the statement for his new audience, the United Nations General Assembly, which he was due to address in a few short days. In the address, Eisenhower would express his deep concern about the pace at which the weaponization of a novel technology was progressing. Stressing the need for all parties to come to the table, Eisenhower laid the groundwork for negotiations, which would establish an organization to help ensure that that weapons technology wouldn't spread. The organization is the IAEA, the weapons technology was nuclear warheads, and the goal was nonproliferation.

Even with the powerful nudge from Eisenhower, it took years for the international community to progress on controlling the flow of this new weapons technology. Over the course of those years, nuclear expertise was infused into policy circles so that those tasked with crafting the rules of the road could understand what it was that they were trying to control. Economists converged on the field, not only to examine decision making around deterrence, but also to look into the markets for goods and services the enabled the creation of nuclear warheads. In March 1970, approximately sixteen years and thousands of work hours after Eisenhower began the process, the Treaty on the Non-Proliferation of Nuclear Weapons went into effect.

In response to the publicity of Stuxnet, the network operations campaign that sabotaged the Iranian nuclear enrichment program, General Michael Hayden, former director of both the Central Intelligence Agency and the National Security Agency, noted that the time we live in "has the whiff of August 1945. Someone, probably a nation-state just used a cyber weapon in a time of peace… to destroy what another nation could only describe as their critical infrastructure"[1]. In 2016, we are in the midst our 1953 moment as leaders across the globe add cyber risk to the list of top threats to global stability.

This article explores the possibility of constraining the spread of malicious offensive cyber capabilities to actors that may be moved to use them outside of the framework of accepted international norms, like rogue states and non-state terrorist or criminal groups[2].

The argument herein is as follows: firstly, the international community has yet to successfully constrain the spread of information. Secondly, the code that supplies the backbone for malicious offensive cyber capabilities is information. Therefore, international policy-makers should explore alternative ideas to

1 | Shinkman, P., Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima, U.S. News, 2013. (online) http://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima.

2 | For the purposes of clarity and consistency, this article uses the term malicious cyber capability. By malicious cyber capability, we do not mean every piece of malware that could be used for offensive purposes. Instead, we use the term to mean a tool designed to allow access to a computer system or network and deliver damage or physical harm to living or material entities.

prevent the spread of malicious capabilities. In examining the details of previous regimes pointed at countering the proliferation of a weapons technology or illicit good, we find that one early step is to place restrictions on testing newly developed capabilities. This report explores the possibility of doing the same for malicious cyber capabilities.

Building a Global Stability Regime for Cybersecurity

Global stability regimes are built on three pillars: norms and laws, deterrence, and arms control. Norms and laws determine what states and other actors in the international system should and should not do by prescribing and describing certain actions and consequences. Deterrence, similarly, serves to appeal to what actors should and should not do via what is called signaling. Contrary to norms, laws, and deterrence, arms control, which often requires that development of norms or international laws in order to be effective, limits what actors can and cannot do by controlling access to capabilities to carry out coercive behavior and create destructive effects.

While it is important to note that not all three of the pillars need be tailored to specific security areas, like cybersecurity or nuclear security, some aspects of each do in order to bring about the implementers' desired effect. In cybersecurity, most, if not all, nation-states have generally agreed to a set of norms that begin to construct the guardrails on either side of the road—indicating what actors *should* and *should* not responsibly do in cyberspace. Deterrence, the second half of the should/should not equation is proving difficult to articulate in cybersecurity terms, but deterrence is perhaps the least context dependent and does not require area-specific or tailored action—especially as the anonymity of attackers or attacking groups decreases. Countless hours of intellectual capital have been poured into deliberations of what actors should and should not do in cyberspace, but we will leave these discussions here.

Instead, with the ever-growing threat that is expanding beyond only nation-state actors, in order to maintain global and regional stability as well as national security, we will consider ways to bind what actors—including, but not limited to states—*can* and *cannot* do. In our view, this does not mean casting aside efforts to codify cybersecurity norms and develop new deterrence strategies; indeed, an effective global stability regime will mix all of these elements. Instead, a renewed focus on limiting the capability of actors can exist in parallel with these efforts.

To effectively limit what effects actors can and cannot produce, the cybersecurity policy community must (1) focus on resilience, or what some call deterrence by denial, and (2) examine ways to limit the availability of destructive tools. This article explores the possibility of constructing a global regime to achieve the ladder of these policy objectives.

> “ Global stability regimes are built on three pillars: norms and laws, deterrence, and arms control.

In this article, we explain why controlling spread of information and computer code is infeasible by exploring how the proposed intrusion software export is in the process of failing and dissecting the spread of encryption technology in the 1990s. Next, we outline what a strategy aimed at constraining the spread of malicious cyber capability might hope to achieve and explore the art of the possible in this context. In doing so, we examine past attempts at constraining the spread of weapons and other illicit goods. Finally, we lay the groundwork for building such a strategy in the absence of export controls on blanket terms like intrusion software, malware, and even “Advanced Persistent Threat Software and related materials.”

What is Possible? Controlling the Export of Information (code)

In late 2014, news broke of a cyber attack that caused a blast furnace at a German steel mill to explode. Occurring between two major cyber attacks with considerable geopolitical narratives—the Stuxnet campaign in Iran and

the disablement of the Ukrainian power grid—the incident in the German steel mill went relatively underreported. Perhaps because the incident is difficult to map to significant geopolitical events or maybe because many in the cybersecurity community that this was a case of espionage gone wrong and the attackers never actually meant to deliver the payload that caused the damage, the incident received relatively little media coverage.

Just as some computer code can execute to make our lives more efficient or secure, conceivably code can execute to make our lives less efficient and less secure. The kinds of code capable of eliciting negative consequences varies drastically in terms of both complexity and effect. The status quo has not reached a point where any malicious cyber capability could reasonably be considered a weapon of mass destruction, as some have suggested[3]. It is widely accepted that computer code has not yet caused the loss of human life, which would seem to be a prerequisite to being considered a WMD. Nonetheless, as security engineer Bruce Schneier notes, "the Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," and "the next president will probably be forced to deal with a large-scale internet disaster that kills multiple people"[4]. These events and statements send a clear signal: it is time to start figuring out how to control these capabilities.

The problem with computer code, and by extension offensive cyber capability, is that it is essentially information. Malicious software, or malware, is the word often used to describe the computer code that attackers use to execute their desired effect. Malware is comprised of several components: propagation[5] methods, software or hardware vulnerabilities, exploits, and payloads.

Propagation methods are the way that outsiders get their code onto a targeted system, and can include things like emails that trick the user into clicking on a link to visit a compromised website or downloading a corrupted file. The pervasiveness, combined with the ease with which one can develop a propagation method and the inherent dual-utility of remote access—many software developers use a propagation method to push security updates—render it a difficult target for controls.

Vulnerabilities are the way in—the crack in the software's armor that allows an attacker to gain access to otherwise-protected systems. These include zero-days, or high-value, undisclosed vulnerabilities that the software's creator is unaware exist. Vulnerabilities are the cornerstone for the construction of malware and are often folded in with other code to develop propagation methods, exploits, and payloads. While vulnerabilities are perhaps the easiest component to isolate and identify, they are likely the toughest to control without severely hindering security. Vulnerability reporting, which could be interpreted as the export of vulnerabilities, should the reporting occur across borders, is essential for the crowdsourcing security model of many software companies and bug bounty programs.

Exploits are software or executable commands that attack targets using the holes provided by vulnerabilities. As with vulnerabilities, some security companies and researchers use exploits as part of their cybersecurity-related products and services. In other words, if the dual-use nature of vulnerabilities presents a hurdle for arms-control, the same argument can be made for exploits.

Payloads[6] are the component that cause damage and are distinct from the delivery method, which the prior three components make up. What differentiates a cyber weapon from an espionage tool or other malware is its destructive payload. The destructiveness of payloads can vary widely and the malware of interest for this article, malware that can help deliver physical destruction (see

3 | Zetter, K., Computer Malware the New 'Weapon of Mass Destruction', Wired, 2008. https://www.wired.com/2008/12/cybersecurity-c.

4 | Schneier, B., The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters, Motherboard, 2016. http://motherboard.vice.com/en_uk/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster.

5 | Herr, T., The PrEP Model: An Introduction, Cyber Security and Privacy Research Institute, The George Washington University, 2014. (online) http://www.cspri.seas.gwu.edu/blog/2014/7/25/the-prep-model-an-introduction.

6 | Hardikar, A., Malware 101 – Viruses, SANS Institute InfoSec Reading Room, 2008, p. 32. (online) https://www.sans.org/reading-room/whitepapers/incident/malware-101-viruses-32848.

Text Box 1), often relies on some of the same parts that espionage tools use, for example a remote access Trojan to allow for persistent access to the targeted system, but in the end manipulate code and a physical system deliver an effect beyond that remote access.

The international community has twice attempted to construct export control regimes to control the spread of information in this context: most recently, with the Wassenaar Arrangement controls on "intrusion software", and, before that, with the 1990s proposals to block the export of encryption technology. In this section, we will explore these case studies and attempt to draw out lessons from each.

Text Box 1:
Building Destructive Payloads

Destructive payloads, like Stuxnet's, which was responsible for slowing nuclear centrifuges in Iran, are precisely tailored to the system they target in such a way that often times a single payload will only deliver its desired effect to a single, specific system. This type of focused design requires an intimate knowledge of the systems being attacked—Stuxnet, for example, targeted the incredibly specific Siemens S7-315-2 PLC (Programmable Logic Controller, a device that controls machine automation). It's worth noting that not all payloads can elicit physical destruction, nor do all payloads necessarily signal intent or specify a target. For example, RawDisk, the tool used to brick a swath of Sony Pictures' machines could be seen as physically destructive as it rendered the computers worthless by deleting all of their data. But wipers, like RawDisk, are less system-specific and can often be deployed against any and all systems that use a certain piece of software or operating system. Nonetheless, particular payloads, when combined with a specific exploit, could only be used for one purpose; the research for the payload and the vulnerability feeding the exploit make it so. Payloads capable of delivering physical damage are time-intensive and hard to create, but also is extremely difficult to identify in development.

The Wassenaar Arrangement: Controlling "Intrusion Software"

States have realized the challenges posed by the acquisition and use of malicious offensive cyber capabilities by non-state groups, like criminal groups and terrorist organizations, and rogue states. In response to this recognition, policy makers have attempted to address the issue via a 41-member multi-lateral arms control agreement called the Wassenaar Arrangement (WA).

Late-2013 additions to the control list of the WA,[7] a 41-member, multilateral arms-control agreement that helps harmonize export control regimes across the world, attempted to slow the spread of some malware under controls on "intrusion software"[8],[9]. Unpacking the intention of this control is nearly as complicated as navigating the United States' export control system itself. In this section, we will do both.

7 | Wassenaar Arrangement, About us, The Wassenaar Arrangement, 2016. (online) http://www.wassenaar.org/about-us.

8 | Garnick, J., Changes to Export Control Arrangement Apply to Computer Exploits and More, The Center for Internet and Society, 2014. (online) http://cyberlaw.stanford.edu/publications/changes-export-control-arrangement-apply-computer-exploits-and-more.

9 | During the same plenary, the Wassenaar delegations also agreed to a related technology control on "IP network surveillance systems". This control, proposed by the French delegation, is targeted at systems that classify, collect, and can inspect all the digital traffic flowing through a network. In this case, the motive for the control (and by extension, what it was meant to do) was clear. Governments entered into negotiations with a clearly defined human rights goal in mind: prevent despots and bad actors from obtaining technology that they could then use to commit abuses domestically. As Carnegie Scholar Tim Maurer notes, "The creation of these new controls set a precedent by adding a human rights component to the Wassenaar Arrangement." The IP network surveillance systems control is the source of some controversy within U.S. industry, but is less relevant to this study than the proposed control on what the WA calls "intrusion software".

The intrusion software control, proposed by the British delegation, was initially framed to focus on "Advanced Persistent Threat Software (APT) and related equipment (offensive cyber tools)"[10]. In the end, the proposed control targets the infrastructure that enables the "generation, operation, delivery of, and communication with" intrusion software, which it defines as "'software' specially designed or modified to avoid detection by 'monitoring tools', or to defeat 'protective countermeasures', of a computer network capable of performing" either extraction or modification of system or user data or the modification of a standard execution path of a program or process[11]. Intuitively, the language of this control appears tailored to address a national security problem, more than a human rights one.

One of the difficulties posed by big bureaucracies (and even small ones), like the UK government that proposed the intrusion software control, is that they represent a system nearly as complex as the international system. In doing so, just as it is difficult for a group of states to build consensus around a policy goal and the measures needed to achieve that goal, it can be difficult for the bureaucracy of a government to align itself around one goal. Where the IP network surveillance systems control clearly sought to prevent human rights abusers from obtaining technology that would enable them to carry out said human rights abuses against their own people, the intrusion software control is far more ambiguous in its intended target and, by extension, its intended effect.

Text Box 2:
The Wassenaar Arrangement at a Glance

The U.S. Department of State lists the WA as a "multilateral nonproliferation export control regime" along-side the likes of the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Australia Group. Wassenaar membership includes most of Europe, Argentina, Australia, Canada, Japan, New Zealand, Russia, South Africa, South Korea, and the U.S. Though not a formal member, Israel implements suggested controls on a voluntary basis.

The primary goal of the WA is to synchronize member-states' export control regimes to limit the sale and trafficking of dual-use technologies—those that could have both a civilian and potential military application. The WA is not a treaty and therefore has no binding power, but member-states agree to establish and enforce export domestic controls on items listed on the WA's control list, which is updated every December. In the past, the WA has been used primarily to harmonize export control regimes relating to conventional, nuclear, chemical, and biological weapons as part of a broader nonproliferation regime for these weapons.

Some in the UK government were motivated by national security concerns—that is to say, the crafters of the control hoped that it would prevent more state and non-state actors from obtaining or building what we refer to as malicious cyber capabilities in this article and what the UK initially called APT software or offensive cyber tools. Other parts of the UK government likely hoped the intrusion software control would serve to help protect human rights by preventing potential abusers from buying malicious tools. The operative point here is that, whether or not the UK government or the UK Wassenaar Delegation was unified in its motivation for the control, some in the UK government sought to prevent the flow of intrusion software for national security purposes. This move represented the first public movement towards countering the proliferation of malicious cyber capabilities.

10 | Reports from the Business, Innovation and Skills, Defence, Foreign Affairs and International Development Committees Session 2013-14 Strategic Export Controls: Her Majesty's Government's Annual Report for 2011, Quarterly Reports for 2011 and 2012, and the Government's policies on arms exports and international arms control issues ; Response of the Secretaries of State for Defence, Foreign and Commonwealth Affairs, International Development and Business, Innovation and Skills, 2013, p. 37. (online) http://www.official-documents.gov.uk/document/cm87/8707/8707.pdf.

11 | Bureau of Industry and Security, U.S. Department of Commerce, Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion Software and Surveillance Items, Federal Register, 2015. (online) https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

Implementation Around the World

Despite this shift in priorities mid-stream, the majority of Wassenaar member states have implemented the proposed technology controls. Japan[12], Australia[13], and the European Union member states[14], and others have successfully crafted controls on both intrusion software and IP network surveillance tools, as outlined by the Arrangement. In addition, Israel, which is not a member of the Wassenaar Arrangement but voluntarily implements most of the controls, has folded the two controls into their export control regime.

Problems with Implementation in the US

Implementation in the U.S. has been slower. Former U.S. Secretary of Defense Robert Gates has described U.S. export controls law as a "byzantine amalgam of authorities, roles, and missions scattered around different parts of the federal government." This "diffusion of authority… results in confusion about jurisdiction and approval."[15] In the U.S., two lists, administered by two different executive departments regulate and control exports: the Export Administration Regulations (EARs), administered by the U.S. Department of Commerce and the International Traffic in Arms Regulations (ITARs), administered by the U.S. Department of State. In simplified terms, the EARs regulate dual-use items and the ITARs regulate "defense articles"[16]. After careful consideration and much intra-agency dialogue, the U.S. Department of Commerce's Commerce Control List (CCL) was selected as the relevant list to implement the controls.

As Tim Maurer, Edin Omanovic, and Ben Wagner note, the U.S. export control system "tends to be quite insular" and is "mostly decided through intra-governmental processes with a limited number of outside experts influencing" the developments. This limited expertise provides input through Technical Advisory committees, which are "comprised of representatives from industry and government" and focus on "dual use-items and technology."[17]

Two Technical Advisory Committees (TACs) provided subject matter input on the implementation of the Wassenaar technology controls: the Information Systems Technical Advisory Committee (IS-TAC) and the Emerging Technology and Research Advisory Committee[18]. Symantec's Michael Maney, a member of the IS-TAC, posits that, "the cybersecurity community was not well represented on the TACs" to provide the necessary insight to government agencies as they proposed the new rules and the outreach was not done "particularly effectively."[19] Whether it was truly a lack of expert voices or whether the expert voices simply went unheeded, the rule proposed by Commerce in May 2015 was fraught with problems. Opposition to the proposed rule surfaced in the private sector and white hat hacking community. The opposition largely focused on two separate but related streams: (1) two restrictive policies ingrained in the U.S. export controls regime and (2) the content of the controls.

In hindsight, in addition to general challenges with the construction of this kind of a security regime for cybersecurity, implementation of the Wassenaar Arrangement's proposed technology controls faced major hurdles in the U.S. because of the concept of a "deemed export" (see text box 3), a policy to deny licenses by default (see text box 4), and the sticky issue of intrusion software, which we will focus on here.

12 | Hoar, S. and Thompson, B., Pardon the "Intrusion"—Cybersecurity Worries Scuttle Wassenaar Changes, Davis Wright Tremaine LLP., 2015. (online) http://www.privsecblog.com/2015/09/articles/cyber-national-security/pardon-the-intrusion-cybersecurity-worries-scuttle-wassenaar-changes.

13 | See Liam Nevill email: Defense and Strategic Goods List.

14 | Modrall, J., European Commission takes action to control exports of cybersecurity tools, Norton Rose Fulbright, 2014. (online) http://www.nortonrosefulbright.com/knowledge/publications/123256/european-commission-takes-action-to-control-exports-of-cybersecurity-tools .

15 | Gates, R., Business Executives for National Security (Export Control Reform), U.S. Department of Defense, 2010. (online) http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1453.

16 | https://www.pmddtc.state.gov/regulations_laws/itar.html.

17 | Maurer, T., Omanovic, E, and Wagner, B., Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age, New America, 2014. https://www.newamerica.org/oti/policy-papers/uncontrolled-global-surveillance-updating-export-controls-to-the-digital-age.

18 | CSIS, Decoding the BIS Proposed Rule for Intrusion Software Platforms, CSIS Strategic Technologies Program, 2015, min. 20:00. (online) https://www.csis.org/events/decoding-bis-proposed-rule-intrusion-software-platforms.

19 | Ibid, min. 21:15.

Text Box 3:
The Deemed Export

In the most basic sense, a "deemed export" is the transfer of knowledge about a restricted technology to a foreign national. BIS defines a deemed export as "An export of technology or source code (except encryption source code) is 'deemed' to take place when it is released to a foreign national within the United States." The release of technology includes when technology is made "available to foreign nationals for visual inspection (such as reading technical specifications, plans, blueprints, etc.); when technology is exchanged orally; or when technology is made available by practice or application under the guidance of persons with knowledge of the technology." The concept of a deemed export poses a particular issue for the export of intrusion software, which is code and therefore essentially information.

Text Box 4:
Denial by Default Policy

The second embedded policy is what some refer to as the default denial policy. In order to export a controlled good to a restricted country the exporter must apply for a license. For the items listed on the CCL, BIS evaluates these license applications. It is BIS' policy to deny any application if any applicable policy requires denial, "even if another policy provides for approval."

The U.S. export control regime is not particularly adept at controlling truly dual-use goods because of this denial by default policy. Defaulting to deny a license works well when the vast majority of uses of a dual-use good are ones you want to prevent. In such a case, it is safe—or at least safer—for commerce to assume that the potential exporter is seeking a license to send the good to an end user who will use it in a way Commerce does not wish it to be used. However, when a good is used predominantly for positive purposes, the restrictiveness of a denial by default system poses problems. While this may not be the case with IP Network Surveillance Tools, as listed by the Arrangement, it does pose problems for the intrusion software control.

Sticky Issue: Intrusion Software

The language of the intrusion software control, as proposed by the Department of Commerce[20], provoked skepticism from the cybersecurity community because the rule removed some of the exclusions and protected categories that were largely present in the proposed rules in other countries[21]. Many in industry and academia fear that the restrictions could also apply to benevolent[22] pursuits[23] like penetration testing and information sharing on vulnerabilities, as the language of the control does not differentiate based on intent[24]. In addition to the concerns of security companies that the controls would restrict their ability to do business[25], security researchers harbored concerns that these controls would prevent penetration testers in countries that implement controls from responsibly reporting vulnerabilities discovered across borders. This failure to consider the full impact of the controls led to a wave of strong criticism from cybersecurity companies and researchers, which focused on the broad brush with which the U.S. proposed implementation paints its restrictions on intrusion software.

As the founder of the Microsoft bug bounty program (and New America Cybersecurity Fellow), Katie Moussouris, noted, the export controls proposed in the U.S.

20 | Bureau of Industry and Security, U.S. Department of Commerce, Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion Software and Surveillance Items, Federal Register, 2015. (online) https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

21 | Op. cit. CSIS, 2015, min. 26:40.

22 | Bratus, S., BIS Public Comment, Dartmouth College, 2015. (online) http://www.cs.dartmouth.edu/~sergey/wassenaar/bis-public-comment-july20-2015.pdf.

23 | Bratus, S., Capelis, D., Locasto, M., and Shubina, A., Why Wassenaar Arrangemnt's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense At Risk—And How to Fix It, Dartmouth College, 2014. (online) http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

24 | Bratus, S., The Wassenaar Arrangement's intent fallacy, Dartmouth College, 2015. (online) http://www.cs.dartmouth.edu/~sergey/wassenaar/wa-intent-fallacy.pdf.

25 | McGuire, C., U.S. Commerce Department Controversial Rule Will Weaken Security Industry and Worldwide Protections, Symantec Official Blog, 2015. (online) http://www.symantec.com/connect/blogs/us-commerce-department-controversial-cybersecurity-rule-will-weaken-security-industry-and-worl.

could deter bug bounty programs by requiring any would-be bug reporter to apply for an export license in order to report the bug across state borders. In other words, if a security researcher in the U.S. were to find a bug in SIMATIC NET PC-software[26], software made by Siemens, headquartered in Germany, the researcher would not be allowed to report the bug to Siemens until she is granted an export license. Google also highlighted the potential issues the controls could pose to communication within multi-national corporations, arguing, "If we have information about intrusion software, we should be able to share [it] with our engineers, no matter where they physically sit."[27]

In addition to potential problems around vulnerability reporting and sharing, comments from industry pointed out that the broadness of the language in the controls would prevent them from conducting core pieces of business designed to help, not hinder, cybersecurity. For example, the controls proposed by BIS in the U.S. would likely restrict the export of the proprietary platforms based on the popular, open source penetration testing platform, Metasploit, which are used widely by White Hat hackers looking for security vulnerabilities to responsibly report[28].

In response to the backlash, the Obama Administration reversed its position[29] on the proposed controls and informed many in the community that they would attempt renegotiate the controls with the WA members, which the U.S. delegation has been attempting to do over the summer, ahead of the WA plenary meeting in December. But even as these renegotiations take place, questions remain as to whether policy-makers have armed themselves with the knowledge necessary to craft a meaningful regime that does no harm to the market for cyber-defensive tools.

In the end, the attempt to construct a nonproliferation control on intrusion software at the WA could be considered a failure. As some in industry have noted, the proposed controls would have "a greater impact on the legitimate work around the world and [wouldn't] really have an impact on who they were actually targeting for the control"[30]. Many of the challenges facing Wassenaar implementers around controlling information also played out in the 1990s in the United States around the so-called crypto wars[31].

General Challenges

Beyond the specific challenges faced by the WA, the construction of a nonproliferation regime for malicious cyber capabilities faces challenges with regard to establishment and enforcement.

First on establishment, countries around the world cannot yet agree on a purpose for such a regime, at a fundamental level. Some place far higher emphasis on the importance of maintaining the functionality of physical critical infrastructure reliant on global networks, calling this cybersecurity. Others take a far more holistic view of security in this space (usually using the term ICT security or information security) and include control of content under their definition of security. For example, using a satellite to broadcast CNN into a territory would not be considered a malicious cyber capability by many in the West, but may be in Russia[32]. This foundational

26 | SIMATIC NET PC-software is a piece of software that can run on the Windows operating system of most PCs and allows human operators to more easily interact digitally with the Programmable Logic Controllers at the core of industrial automation.

27 | Martin, N., and Willis, T., Google, the Wassenaar Arrangement, and vulnerability research, Google Security Blog, 2015. (online) https://security.googleblog.com/2015/07/google-wassenaar-arrangement-and.html.

28 | Ellis, J., Response to the US Proposal for Implementing the Wassenaar Arrangement Export Controls for Intrusion Software, Rapid-7Community, 2015. (online) https://community.rapid7.com/community/infosec/blog/2015/06/13/response-to-the-us-proposal-for-implementing-the-wassenaar-arrangement-export-controls-for-intrusion-software .

29 | Barth, B., Executive branch concedes Wassenaar Arrangement must be renegotiated, not revised, SC Magazine, 2016. (online) http://www.scmagazine.com/executive-branch-concedes-wassenaar-arrangement-must-be-renegotiated-not-revised/article/481020.

30 | Op. cit. CSIS, 2015, min. 22:45.

31 | Omanovic, E., Open-source software: Export Uncontrollable, Privacy International, 2013. (online) https://www.privacyinternational.org/node/344.

32 | Kanuck, S., Sean Kanuck on Deterrence and Arms Control in Cyberspace, The Berkman Klein Center for Internet and Society, 2016, min. 47:30. (online) https://www.youtube.com/watch?v=N7VgvPB-3DU.

disagreement over what constitutes security in this context has led to an uncertainty about applications of international law.

Much of this uncertainty hinges on linguistic ambiguities. However, the ambiguities do not stop at defining what we want to secure. Indeed, many disagree over what constitutes a weapon. Is the satellite described in the previous paragraph a weapon, or must a weapon be used to directly elicit physical damage or loss of life, as we contend? And what represents an attack? Is a simple data breach an attack, as has been popularized in news media? Or must an attack use a weapon, as we describe it[33]?

International regulation cannot keep pace with rapid changes in technology. For example, in the counter-narcotics space certain compounds are criminalized. However, as new drugs based on new compounds develop, it takes international regimes and law months and often times years to catch up[34].

Second, questions remain about the enforceability of a nonproliferation regime aimed at malicious cyber capabilities. The scope of conflict, potential actors, potential targets, and potential impacts is massive[35]. To compound this problem, the nature of cyberspace and private sector ownership of much of the infrastructure limits sovereign control over the attack surface[36]. Furthermore, the tools and activities themselves are largely unobservable. Whereas satellites or other tools are likely to detect a controlled nuclear explosion, testing of malicious cyber tools often takes place in a laboratory[37]. In some sloppy cases, there is reason to believe that some testing of malicious cyber capabilities has taken place in the wild, as is arguably the case with the 2014 German steel mill incident. Despite the transnational and increasingly threatening nature of cyber attacks, states have yet to develop good mechanisms for cooperation. This could be due, in part, to disincentives for the victim of a cyber attack to verify (or even acknowledge) an attack occurred.

33 | Ibid, min. 52:20.
34 | Ibid, min. 52:49.
35 | Ibid, min. 54:52.
36 | Ibid, min. 55:20.
37 | Ibid, min. 56:05.

“ Despite the transnational and increasingly threatening nature of cyber attacks, states have yet to develop good mechanisms for cooperation.

In verifying and attributing an attack, the victim reveals its own intelligence and capabilities[38].

The Wassenaar Arrangement’s “intrusion software” control and the crypto wars of the 1990s suggest that controlling the flow of code is infeasible. Thus, we are forced to look elsewhere for more creative interventions.

What Are We Trying to Achieve?

Before policy makers dive in to the choppy waters of building an international regime, it is important to clarify a number of considerations. These considerations will be unpacked in greater detail in the final section of this article, but they also provide a convenient framing for readers to contemplate as they progress through this text.

As a first step, a state or group of states must decide what it is that they are trying to achieve with a non-proliferation regime. In a very basic sense, this means answering a central question: What sort of effect do we desire to stamp out? Once enumerated, this high level goal informs decisions around what type of tool or tools need be controlled and what groups of people need be prevented from obtaining or developing said tools. It then becomes the job of those tasked with regime construction and implementation to understand the technology they are trying to control, how that technology is acquired or developed, who the relevant stakeholders are, and all of the available options for controlling the good or service. There need not be international consensus around any of these questions at the beginning. Building this consensus and generating international

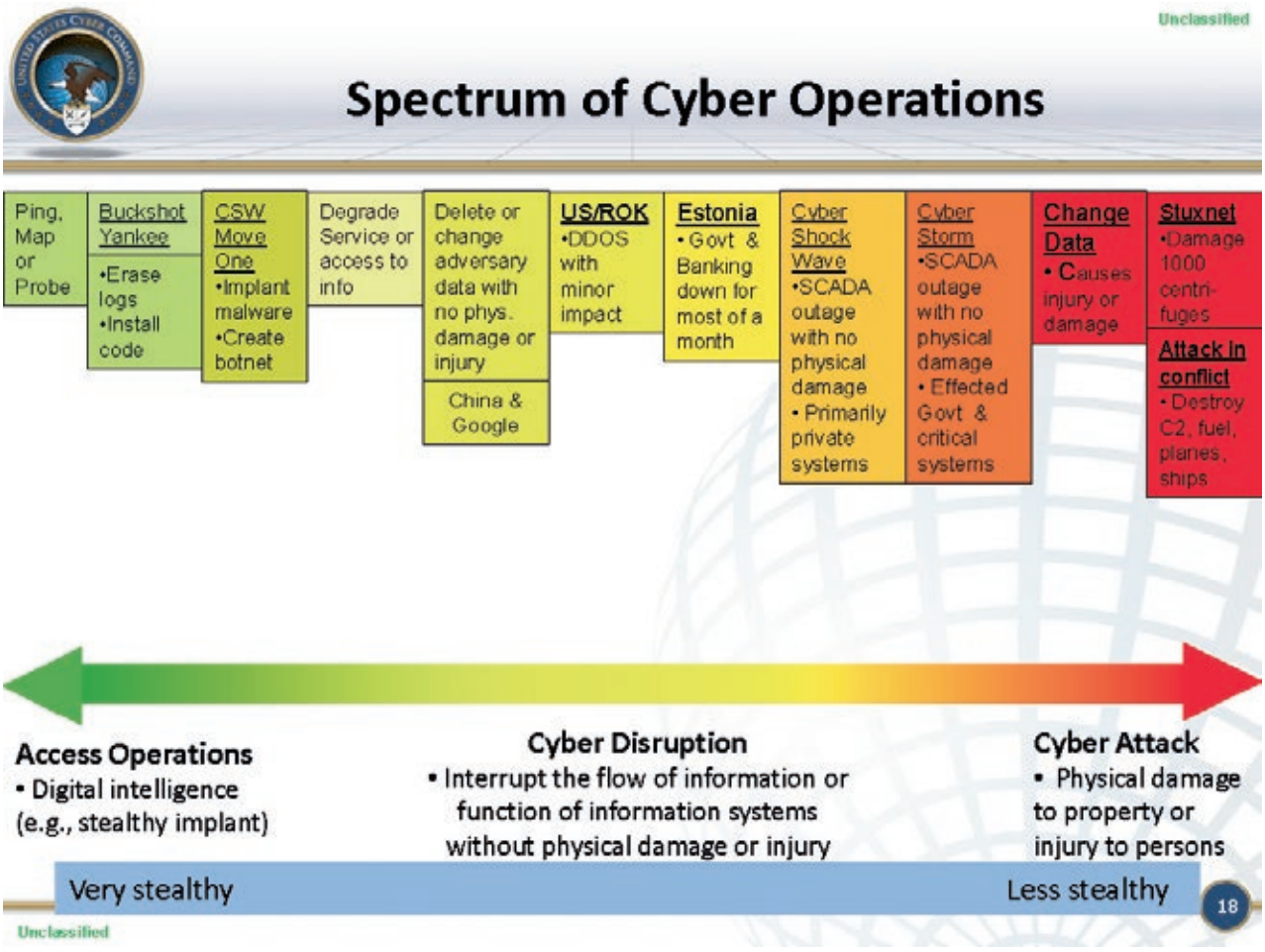
38 | Ibid, min. 56:45.

buy-in will likely be the part of a select group of thought and policy leaders.

Unclassified documents from U.S. Cyber Command outline a spectrum of cyber operations based on past events (Figure 1). In this article we posit that the international community should focus on preventing effects on the far right end of this spectrum, which Cyber Command has labeled "Cyber Attack". To be clear, an arms control, nonproliferation, or counterproliferation regime is unlikely to cover the entirety of the wide swath of tools that many commentators refer to as malicious cyber capabilities, and it is paramount that any crafted regime does not hinder the development and spread of cyber-defensive technologies and services.

Figure 1. Spectrum of Cyber Operations. Source. U.S. Cyber Command

In this context, we use the term arms control to mean limit the number or kind of a certain classification of weapon, nonproliferation to mean to prevent or limit the spread of a certain classification of weapon, and counter proliferation to mean to limit the utility of a certain classification of weapon. In an arms control arrangement, governments agree to not produce or stop producing a certain weapon, or reduce the size of their existing arsenal. Counterproliferation, coined by the Clinton Administration of the 1990s, involves governments changing what they buy to combat the threat, plan to fight wars differently, and change how they collect intelligence and what intelligence the collect[39]. A nonproliferation regime involves governments agreeing to not sell a weapon to a country without that weapon and to not help (through the sale of component parts or the transfer of knowledge) a country without a weapon develop that weapon.



39 | Aspin, L., Remarks to the National Academy of Science, FAS.org, 1993, (online) http://fas.org/irp/offdocs/pdd18.htm.

Regime Type	Explanation
Arms Control	Governments agree to not produce or stop producing a certain weapon
Counterproliferation	"Directly forestalling, rolling back, or eliminating efforts to proliferate" a weapon, and preventing an actor that has already obtained the weapon "from realizing any benefit from owning or employing these weapons."
Nonproliferation	The "means and methods for preventing the acquisition, transfer, discovery, or development of materials, technology, knowledge, munitions/devices or delivery systems related to" a weapons technology.

Figure 2. Typology of arm control strategies as described by US Secretary of Defense Aspin. Source. Aspin's Remarks to the National Academy of Science, 1993.

From here, we will focus on the possibility of constructing a regime akin to a nonproliferation regime, as outlined above. We propose that any effort at crafting a regime should focus on tools with potential to cause physical destruction or loss of life (weapons), because, in addition to having the highest potential impact, they are prohibitively difficult to build. This does not mean attempting to control every piece of malware, but rather the upper echelon of tools. The analysis that follows is based on that assumption, but is tailored for select application in lieu of this assumption or goal.

What Next? Learning From the Past

So how might the international community go about restricting the development and spread of malicious cyber capabilities? Nonproliferation regimes exist and have been effective models for controlling the flow of certain destructive technologies. Although cybersecurity-policy experts often look on analogies to nuclear, chemical, and biological weapons with disdain, the broader policy community gravitates to easy analogues to understand convoluted issues. On a number of levels, these analogies do not work, though does not mean that some illuminating parallels cannot be drawn and lessons cannot be learned.

Preventing actors from developing and deploying malicious cyber capabilities seems difficult, if not impossible, and it may be tempting to think tools of like Stuxnet as exceptional in their uncontrollability. A number of academics and policy-makers, following the maxim that "metaphor, rather than experience, is the currency of discussion,"[40] have tried to apply different analogies to cyber in order to explain some of the nuances of cyber conflict and, in some cases, explore ways the weapons could be controlled. Nuclear, chemical, and biological (NCB) are most often compared to cybersecurity. In this section, we will delve into lessons for policy-makers from these regimes, as well as regimes focused on stemming the flow of small arms and narcotics, that can and cannot apply to cybersecurity. Although some valuable lessons can be drawn from these analogies, it is important to note that they are not perfect.

Lesson 1: Constructing a nonproliferation regime is hard

The first lesson that policy-makers must heed is that the construction of a security regime – and particularly of a nonproliferation regime – is arduous. It takes time, subject matter expertise needs to be developed and infused into policy circles, hurdles like crafting a viable verification or inspection regime must eventually be overcome, and an understanding of the above and below ground markets for relevant goods and services must be developed and leveraged.

For the policy-makers involved in the process, patience is paramount. In his 1953 "Atoms for Peace" speech, Eisenhower noted the imperativeness of patience, saying:

40 | Libicki, M., Defending Cyberspace and Other Metaphors, National Defense University, 1997, p. 65.

In this quest, I know that we must not lack patience. I know that in a world divided, such as ours today, salvation cannot be attained by one dramatic act. I know that many steps will have been taken over many months before the world can look at itself one day and truly realize that a new climate of mutually peaceful confidence is abroad in the world[41].

> “In order to craft a regime that both has the desired effect and minimizes the negative externalities, a deep understanding of the technologies in question must be infused into the policy process.

Eisenhower's words ring equally true today in the context of cybersecurity. As Sean Kanuck, formerly of the U.S. National Security Council and a member of the U.S. delegation to the UNGGE, notes, “Now a' days if you're going to get a treaty, [the process] is measured in years – maybe longer, decades”[42].

As we've witnessed in the past, negotiation processes around these sorts of regimes are generally long, drawn-out, and controversial. The NPT took nearly 20 years to craft from its early beginnings in 1957 to end and nations continued to iterate on the overarching regime until the mid-1990s with the CTBT. Similarly, Negotiating the surprise inspection provision of the CWC during the tensions of the Cold War was incredibly difficult diplomatically, but ultimately fruitful.

Policy-makers must also accept that the process of building a regime will not be easy. As demonstrated by the shortcomings of the Wassenaar Arrangement, it is possible that the international community will not be able to simply transpose an existing model or models for restricting the flow of goods on top of the cybersecurity problem. Instead, it is far more likely that new and innovative models will need to be built to address the challenge.

In order to craft a regime that both has the desired effect and minimizes the negative externalities, a deep understanding of the technologies in question must be infused into the policy process. Previous regimes have often incorporated technical expertise through institutionalized mechanisms. Physicists who understood the technology and therefore grasped the gravity of the subject made the progress of the NPT, from hard initial negotiations to eventual ratification, possible. The IAEA History Research Project describes nuclear scientists at the forefront of the movement for an international nuclear control agreement[43]. The founding document of the Union of Concerned Scientists (UCS), which was founded by MIT personnel, begins: “Misuse of scientific and technical knowledge presents a major threat to the existence of mankind”[44]. While the cybersecurity threat may not be existential, as the nuclear threat described by the UCS the risks should not be ignored.

Lesson 2: Control something other than information and code.

As the crypto wars and the initial movement around intrusion software controls shows, controlling code, which is simply a form of information, may be prohibitively difficult if not impossible. To address the issue, policy makers must infuse the policy process with subject matter expertise to build a better understanding of how malicious capability is bought, developed, maintained, and deployed. Relatedly, policy makers should renew focus on limiting the means to develop tools as much as

41 | Eisenhower, D., Atoms for Peace, International Atomic Energy Agency, 1953. (online) https://www.iaea.org/about/history/atoms-for-peace-speech.

42 | Op. cit. Kanuck, 2016, min. 53:03.

43 | IAEA History Research Project, The Creation of the IAEA, Universitat Wein, 2016. (online) http://iaea-history.univie.ac.at/the-iaea-at-sixty/the-creation-of-the-iaea.

44 | Union of Concerned Scientists, Founding Document: 1968 MIT Faculty Statement, Union of Concerned Scientists, 2016. (online) http://www.ucsusa.org/about/founding-document-1968.html#.V6tI9FUrLct.

(or more than) preventing the spread of finished tools. In order to achieve this goal, policy-makers should consider the development of grades or schedules for dual use goods that are integral to the development of capabilities. Finally, an early step taken by nuclear non-proliferation efforts was to attempt to control the space within which tests could take place. In order to construct malicious cyber capabilities that will have physical effects, attackers will generally need to purchase and construct a mirror version of the system they wish to impact. A focus on controlling the availability of such test spaces could be an initial step towards limiting the spread of these capabilities more broadly.

> “ Policy-makers should consider the development of grades or schedules for dual use goods that are integral to the development of capabilities.

Lesson 3:
Address the issue in bite-sized chunks.

The final takeaway for policy-makers needs to be to focus on specific verticals and combating specific effects in order to address the issue in bite-sized chunks. One international regulation is not going to fix the problem of the spread of malicious capability. Instead, a security regime will require a suite of policy interventions, many of which are pointed at specific aspects of the problem, in order to address the nuanced differences between securing the likes of a power grid and securing government databases.

Conclusion

In 2013, government delegations to the Wassenaar Arrangement attempted to construct international regulation that would constrain the flow of malicious cyber capabilities to non-state actors and rogue governments in the form of a proposed export ban on “intrusion software”. A strategy focused on constraining what bad actors are able and unable to do is integral to a security regime and complementary to ongoing processes to develop and implement clearer international norms and laws around the use of cyberspace by state and non-state actors.

Constructing a strategy to constrain the spread of malicious cyber capabilities is, conceptually speaking, a good idea. However, implementation of the Wassenaar controls in the United States and around the world has posed very real challenges and could have negative impacts on the global flow of defensive cybersecurity technology and services, thereby materially diminishing cybersecurity around the world. For these reasons and more, it is time to wipe the slate clean and consider other ways to achieve the same strategic goal of preventing malicious cyber capabilities from falling into the hands of groups and individuals who the international community cannot reliably expect to adhere to principles, norms, and laws that would otherwise constrain their behavior. ■

Bezpieczeństwo i gwarancja dostaw

Dywersyfikacja źródeł dostaw to bezpieczeństwo energetyczne kraju i komfort naszych Klientów

Wiemy, że zróżnicowanie źródeł zasobów i inwestowanie w nowe przedsięwzięcia wpływają na stabilność dostaw. Dlatego nasze cele strategiczne dotyczą wzrostu wydobycia ropy i gazu, a bezpieczeństwo i jakość to dla nas wartości nadrzędne.

PGNiG

CYBERSEC HUB

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum – CYBERSEC, one of the main public policy conferences on cybersecurity.

We are open to those who want to build the CYBERSEC community with us. Whether you are in academia, a CEO, an investor or the owner of a startup, you are invited to become an important part of our network. If you are interested in the project visit our website www.cybsersechub.eu or contact us at cybersechub@ik.org.pl.

THE KOSCIUSZKO INSTITUTE

ANALYSIS

THE NEW DIMENSION OF STATE SECURITY: CENTRALLY COORDINATED ACTIVITIES: THE MILITARY DIMENSION

LT CDR WIESŁAW GOŹDZIEWICZ
is Legal Adviser to the NATO Joint Force Training Centre in Bydgoszcz and Expert of the Kosciuszko Institute (Poland). Lt Cdr Wiesław Goździewicz provides legal advice and training on the practicalities of the application of international humanitarian law and legal aspects of military operations. He served at the Public International Law Division of the Legal Department of the Ministry of National Defence. Commander Goździewicz (Polish Navy) joined the Armed Forces as a junior legal officer, at the 43rd Naval Airbase in Gdynia. He is a graduate of the Faculty of Law and Administration of the University of Gdańsk.

Cybersecurity is a multi-faceted and cross-sectoral phenomenon that requires the involvement of the various sectors – military, civil, public and private – to counter all foreseeable threats.

It is also an area in which there is a possibility and a vital need to engage with both the industrial sector and academia as the potential suppliers of modern software and hardware solutions. There are companies in the world specialised in providing state customers with cyber tools, including the offensive ones.

As part of a more broadly understood concept of information security, cybersecurity will interpenetrate other domains, including the physical security of the network infrastructure. Cybersecurity is not possible without ensuring secure communications channels, including classified (secret) communications, and properly secured ICT networks – both confined, isolated from the Internet, and those connected to the Internet. In the latter case, effective safeguards are particularly important, such as data diodes controlling the flow of data between a protected network and the Internet.

The resolutions of the two recent NATO summits

Newport:

- Cyberattack can trigger Article 5 of the Washington Treaty;
- International law applies to cyberspace;
- Cyber operations must comply with international law.

Warsaw:

- Cyberspace recognised as a fully-fledged operational domain;
- NATO members must build effective cyber defence capabilities;
- Cyber Defence Pledge;
- Obligations under Article 3 of the Washington Treaty include cyberspace.

Versatile cyber capabilities

Obviously, cyber defence capabilities must include passive measures protecting military ICT infrastructure (or the part of the civilian ICT infrastructure used for military purposes) from unauthorized access or even hostile activities intended to disrupt military ICT systems. They must also comprise measures enabling the secure and encrypted exchange of information between authorised network users. It is in the interest of the Ministry of Defence to ensure that the systems protecting the military network from unauthorized access or attempts to break into these networks as well as encryption algorithms are unique solutions, relying on commercial products to the minimum extent possible.

Regardless of the domain, effective and robust defence requires the availability of offensive measures in order to run active defence operations and launch counter-attacks, or retaliatory "hacking" ("hacking-back") of the opponents' systems and, if necessary, to launch a pre-emptive cyberattack.

Poland admits more or less openly to seeking offensive cyber capabilities[1]. In 2013, the National Centre for Research and Development in Poland announced a competition for "Developing software and hardware solutions for conducting information warfare [...]" including "[taking over] control over network devices [...] and [the disintegration of] communication nodes by deliberately changing their operating parameters or deactivating selected functions." Further, we read that "[i]n order to take over components of the enemy's network, it is necessary to install software (malware) and electronic equipment either openly or covertly [...]" and, that "[...] creating one's own military botnets [...]" was being predicted[2]. The estimated value of this project was over PLN 6.5 million (USD 1.7 million).

Commercially developed malware FinFisher is said to be used by intelligence agencies in several countries, allegedly including the Czech Republic and Slovakia[3]. Furthermore, the German secret services are believed to have been using commercially delivered malware R2D2 for several years[4].

The Technical Modernisation Programme (TMP) of the Polish Armed Forces for the years 2017–2022 stipulates that the Polish army will allocate 1% of the total TMP's resources, which amounts to approximately PLN 1 billion (USD 0.3 billion) in total, to the development of its cyber capabilities in the period 2017–2019, as well as throughout the five-year period covered by the TMP. Although this figure looks impressive nominally, it pales in comparison with the funds designed for other priority programmes, such as the modernisation of air defence, for which the Polish Ministry of National Defence intends to allocate 14% of the TMP's value in the years 2017–2019, and a total of 24% in the entire five-year period. For the development of mechanised and armoured infantry, the Ministry is planning to allocate 14 and 20% respectively[5].

Good practices

Building effective cyber capabilities requires broad cooperation of the Ministry of Defence and the Armed Forces, both with national and international partners. It is necessary to establish mechanisms for coordination and the exchange of information with civilian authorities and entities engaged in the country's cyber defence, including private sector, most notably the operators of critical infrastructure systems.

The importance of such cooperation has been appreciated by many states. For example, Estonia's Cyber Security Strategy 2014–2017 provides for the creation of conditions to facilitate the organisation and provision of cybersecurity training, workshops and research, as well as to intensify cross-sectoral activities. In addition, given the mutual dependencies and connections (including physical networks) between infrastructure and ICT services, this document recognises that the cooperation among public, private, and academic sectors is essential to building cybersecurity in a coordinated manner[6].

The French digital security strategy formulates similar theses, but it goes a step further by suggesting, just like the present study, that it is necessary to promote the competitiveness of the domestic cybersecurity industrial and research sectors in order to ensure national digital sovereignty. France is committed to fostering innovation and a research-friendly environment by mobilising and coordinating all available public and private resources to give French cybersecurity solutions competitive advantage, which in effect will tangibly benefit both the private sector and the state[7].

1 | Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, National Security Bureau, 22 January 2015, ISBN: 978-83-60846-25-4, p. 9.
2 | Own translation, http://www.ncbir.pl/gfx/ncbir/pl/defaulto-pisy/575/6/1/polaczony.pdf, p. 42–46.
3 | WikiLeaks ujawnia klientów rządowego szpiegowskiego oprogramowania FinFisher, 2014, [online] https://niebezpiecznik.pl/post/wikileaks-ujawnia-klientow-rzadowego-szpiegowskiego-oprogramowania-finfisher/?similarpost (access: 11/05/2017).
4 | Niemiecka policja infekuje rządowym trojanem (R2D2), 2011,[online] https://niebezpiecznik.pl/post/niemiecka-policja-infekuje-rzadowym-trojanem-r2d2/ (access: 11/05/2017).
5 | Dmitruk T., Projekt nowego Planu Modernizacji Technicznej, 2016, [online] http://dziennikzbrojny.pl/artykuly/art,2,4,10262,armie-swiata,wojsko-polskie,projekt-nowego-planu-modernizacji-technicznej (access:11/05/2017).
6 | Cyber Security Strategy 2014-2017, Estonian Ministry of Economic Affairs and Communication, p. 7.
7 | French National Digital Security Strategy, Agence nationale de la sécurité des systèmes d'information (ANSSI), 2015, [online] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, pp. 30-31 (access: 11/05/2017).

The NATO-Cyber Industry Partnership (NICP) can serve as a model for cooperation between academia and the industrial sector. The partnership is based on a legitimate assumption that close cooperation between the contracting authority (NATO) and the supplier (the industry) is the key to streamlining cybersecurity solutions, while the inclusion of the academic sector in this cooperation will grant access to the latest achievements in science and technology.

The NICP brings together NATO institutions, national CERTs and industry representatives of NATO Member States, including medium- and small-sized IT companies, as well as academic centres. Facing common cybersecurity threats and challenges, all these actors share the belief that cooperation and exchange of information, notably with regard to the latest R&D solutions developed by private business and research centres, can significantly accelerate NATO's efforts to develop robust cyber defence capabilities[8].

As part of the NICP framework, the NATO Communications and Information Agency (NCIA) has created Information and Cyber Incident Coordination System (CIICS), the development of which was contracted to the Rhea Group, the Belgian subsidiary of the Canadian ADGA Group[9]. With an annual budget of EUR 600 million (USD 657.3 million) for ICT infrastructure projects[10], the NCI Agency is planning to spend between 2016 and 2019 a total of about EUR 3 billion (USD 3.3 billion) on a variety of IT projects in support of command and control systems as well as satellite communications, air defence, and cyber defence systems[11].

Examples of cyber defence procurements include:

- The implementation of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC); contract worth EUR 134,353.77 (USD 147,190.36) was awarded to SELEX Communications SpA;
- The implementation of the NCIRC interface at Ramstein missile defence unit; contract worth EUR 411,173.64 (USD 450,458.50) was awarded to SELEX Communications SpA;
- The installation of the Active Network Electronic Security System – ANWI ESS for NCIRC; contract worth EUR 352,166.22 (USD 385,813.32) was awarded to SELEX SpA;
- TrendMicro license renewal for NCIRC; contract worth EUR 101,481.02 (USD 111,176.84) was awarded to Insight Technology Solutions Belgium Inc.;
- McAffee license renewal for NCIRC; contract worth EUR 498,627.34 (USD 546,267.80) was awarded to UNI BUSINESS CENTRE B.V.;
- The central purchase of TEMPEST level B workstations; contract worth EUR 1,662,375.58 (USD 1,821,204.31) was awarded to Airbus Defence and Space AS;
- The purchase of communications and IT equipment for the NATO Force Integration Units – NFIUs; contract worth EUR 2,762,779.00 (USD 3,026,743.82) was awarded to Airbus Defence and Space AS;
- The purchase of cryptographic equipment for NATO's communication infrastructure; contract worth EUR 941,334.89 (USD 1,031,273.06) was awarded to Thales Norway AS12.

8 | Who will be involved in the NATO Industry Cyber Partnership?, [online] http://www.nicp.nato.int/nicp-stakeholders/index.html (access: 11/05/2017).
9 | Tigner B., NATO tests cyber alerting tool, [online] http://www.nicp.nato.int/nato-tests-cyber-alerting-tool/index-2.html (access: 11/05/2017).
10 | Why bidding on NATO contracts can boost your bottom line, [online], http://tradecommissioner.gc.ca/canadexport/157947.aspx-?lang=eng (access: 11/05/2017).
11 | NATO announces 3 billion EUR investment in defence technology, 2016, [online] https://www.ncia.nato.int/NewsRoom/Pages/160726_Announcement_3billion_investments.aspx (access: 11/05/2017).

Possible directions for public-private cooperation

The cooperation between public, private, and academic sectors may considerably reduce the duration of research and development work, provided that appropriate information exchange and sharing mechanisms are created in the first place.

Within the NICP framework (see NCIP case study), such mechanisms function on the basis of Industry Partnership Agreements (IPAs) that the NCI Agency concludes with the industrial sector. The Agency has entered into such agreements with FireEye or RSA Security, to name just a few. The aim of the IPA is to allow for rapid exchange of information on cyber threats in order to improve the situational awareness of the parties to the agreement and to strengthen the protection of their networks.[12]

Mutual benefits yielded by the cooperation among the military, industrial partners and academia are not to be underestimated, especially when this cooperation is extended to include national entities. It will:

- enable domestic companies and academic centres to obtain R&D funding to develop solutions requested by the Ministry of Defence.
- allow for customising the solutions being developed by the industry and academic sectors to the specific needs of the contracting authority.
- help increase the security of the designed solutions and systems.

Relying on national entities in the industrial and academic sectors to develop cyber capacities, particularly cryptanalytic and cryptographic solutions, will help create truly secure products and services. This can be done by drafting the terms and conditions of the procurement in such a way as to oblige the author of the solutions to make the contracting authority the sole recipient and user of the source codes and solutions they create. The most important aspect here is to become less dependent on widely available commercial products that are often riddled with security vulnerabilities, often left there deliberately by the manufacturers, as was the case with the RCS system purchased by the secret services in a number of countries, including the Polish Central Anti-Corruption Bureau. Authors of commercial solutions reluctantly (if at all) grant their customers access to the software source codes, and often sell them as the so-called "black box" that allows for no user modifications or enhancements. The lack of access to source codes can effectively render the identification and elimination of potential security vulnerabilities impossible.

Manpower problems

It is impossible to think of building cybersecurity potential without harnessing national human capital. The military structures will "own" this human capital only to a limited extent – the vast majority of cybersecurity experts will be absorbed by the civil sector, where the demand for these professionals is virtually unlimited. It is therefore necessary to create systemic solutions to either attract professionals to state institutions, including the military, or to put them under mobilisation assignment programmes to be deployed in the event of a crisis or an armed conflict, when strengthening the state's defence capabilities, including cyber military capabilities, becomes absolutely critical. Examples of such solutions can be found in France where Cyber Civic Reserve (Reserve Citoyenne Cyber)[13] has been launched or in Estonia, where the Cyber Defence Unit of the Estonian Defence League has been incorporated into the national defence system, giving the entire Estonian Defence League the status analogous to that accorded to the Armed Forces of Estonia in the event of an armed conflict[14].

Israel stands at the opposite extreme. To date, its defence forces are based on general conscription, which also includes women. Set up to conduct cyber operations, Unit 8200 brings together experts being both

12 | Réserve citoyenne cyber: une démarche originale, 2013, [online] http://www.defense.gouv.fr/actualites/communaute-defense/reserve-citoyenne-cyber-une-demarche-originale/(language)/fre-FR (access: 11/05/2017).

13 | Réserve citoyenne cyber: une démarche originale, 2013, [online] http://www.defense.gouv.fr/actualites/communaute-defense/reserve-citoyenne-cyber-une-demarche-originale/(language)/fre-FR (access: 11/05/2017).

14 | The Estonian Defence League Act, 2013, [online] https://www.riigiteataja.ee/en/eli/525112013006/consolide (access: 11/05/2017).

professional soldiers and conscripts. When asked about the human capital and the pay gap between the officers and non-commissioned officers and privates engaged in cyber operations, the former head and architect of the unit, Brig. Gen. Danny Bren said that the main motivation behind the decision to remain on active duty in Unit 8200 is after all the desire to face the challenges the service offers[15].

The Israel Defense Forces scout universities for young candidates who have exceptional analytical skills and at the same time can work as true team players to serve in Unit 8200. As part of the compulsory military service, instead of learning the drill, weapon handling or tactics, successful candidates undergo training in Unit 8200's comfortable, air-conditioned facilities where they learn how to collect intelligence, use state-of-the-art electronic surveillance or data mining techniques. The skills acquired in training have also helped ex-8200 soldiers to succeed in the commercial market[16]. They are often the masterminds behind establishing such companies as Check Point, CloudEndure, CyberReason, ICQ, LightCyber, the NSO Group, Palo Alto Networks, indeni, NICE, AudioCodes, Gilat, outbrain, Leadspace, EZchip, Onavo, Singular, CyberArk or Fortscale. The Israeli army has heavily invested in its professionals who, capitalising on the knowledge gained in Unit 8200, have often succeeded in commercial cybersecurity business. They remain allocated to mobilisation assignment programmes, and are regularly called up for reserve training during which they can use their knowledge and experience gained both in military service and subsequent business activity.

Certainly, such solutions will also require an appropriate training system to be created in order to enable these civilian specialists to phase in relatively smoothly and get accustomed to operating in hierarchical state structures. One of the possible solutions is to announce volunteer "conscription" of professionals to participate in military and civilian crisis management exercises and trainings. Taking into account the salary ranges in the Polish Ministry of National Defence, it is quite safe to assume that in most cases civilian specialist will not consider the financial incentive as the main factor when taking decision to engage in activities to strengthen national cybersecurity. In accordance with the provisions of the Collective Labour Agreement for Employees of Military Budgetary Sector Entities[17], the maximum salary of the Ministry civil service personnel is PLN 8000 gross (USD 2083.82). However, it is highly unlikely that cybersecurity professionals will earn the highest salary given the hierarchical structure of civilian posts in the Ministry of National Defence.

The emoluments for reservists who are called up for military exercise do not look particularly attractive either. The net salary for a 30-day exercise amounts to PLN 2100 (USD 547) for a private, PLN 2512.50 (USD 654.45) for Master Corporal, and PLN 3150 (USD 820.50) for Second Lieutenant. Lieutenant Colonel of the reserve can receive about PLN 5600 (USD 1458.68) for a 30-day exercise[18], whereas his German counterpart about EUR 3500 (USD 3834.40) plus extras for possessing qualifications and skills particularly useful for the army. The salaries offered by the Polish Ministry of National Defence are hardly competitive compared to the private sector offerings, which was repeatedly emphasized (also by the representatives of the Polish government) at the Polish Cybersecurity Forum in 2016[19] and the European Cybersecurity Forum in 2015[20].

An option worth considering is to search for specialists of the young generation who stand out in various competitions or hackathons, thus confirming their knowledge and skills that may be useful from cybersecurity perspective.

15 | EWulman S., IDF unveils new cyber defense HQ, 2016, [online] http://www.ynetnews.com/articles/0,7340,L-4820035,00.html (access: 11/05/2017).

16 | Tendler I., From The Israeli Army Unit 8200 Is Silicon Valley, 2015, [online] https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/ (access: 11/05/2017).

17 | http://www.wbe.wp.mil.pl/plik/file/akty/oslony/akt_199.pdf (access: 11/05/2017).

18 | http://sandomierz.wku.wp.mil.pl/pl/7373.html (access: 11/05/2017).

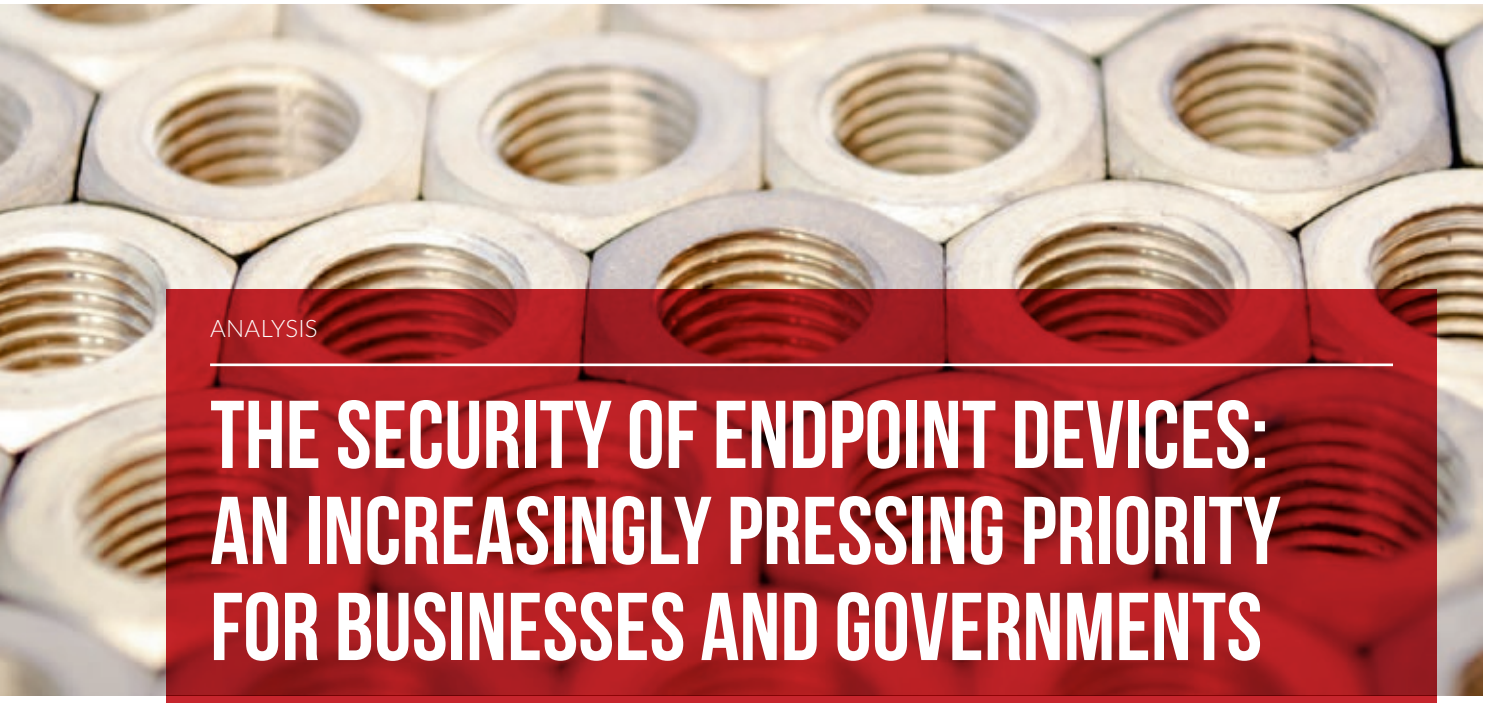
19 | CYBERSEC PL 2016 Rekomendacje, 2016, [online] https://cybersecforum.pl/files/2016/06/rekomendacje_cspl2016_pl.pdf, (access: 11/05/2017), pp. 3-4, 10-11.

20 | CYBERSEC 2015 Rekomendacje, 2015, [online] https://app.box.com/s/o0nb9edtybgxqo9apkjxuium2m6vq9gy, (access: 11/05/2017), pp. 12, 16, 21.

Increasing the number of such initiatives, both nationally and internationally, is paramount to effectively address the problem[21].

In order to maximally utilise the human capital, without "pulling it out" of the work environment, cooperation with cybersecurity entrepreneurs willing to share their potential to enhance the state's cyber defence capabilities should be considered. Such cooperation could include participation in dedicated cyber defence exercises. There have been cases of entrusting private companies with conducting security checks, including penetration tests of the ICT systems owned by ministries of defence. Another scenario to consider is to utilise the potential of companies and entrepreneurs associated in organisations similar to Polish Civic Cyber Defence, both by involving them in intersectoral and interministerial cybersecurity exercises and requesting them to conduct penetration tests or simulated cyberattacks on key ICT systems. These entrepreneurs could be engaged in developing effective methods and techniques to secure critical ICT systems by tapping into their experience in repelling cyberattacks on their own systems. ■

21 | Ibidem, p. 21.



ANALYSIS

THE SECURITY OF ENDPOINT DEVICES: AN INCREASINGLY PRESSING PRIORITY FOR BUSINESSES AND GOVERNMENTS

GIULIA PASTORELLA
leads HP's Government Relations in the UK, Italy and the Nordics since 2015. Based in London, she works in close collaboration with the HP Security Labs in Bristol, where HP's cyber security research is carried out. Before joining HP, she worked as a public affairs consultant between London and Brussels, and as a university contract lecturer in Political Science. She holds a PhD in Comparative European Politics from the London School of Economics (LSE), a double Master's in European Affairs from Sciences Po and the LSE, and a BA in Philosophy and Modern Languages from Oxford University.

We live in a hyper-globalised and hyper-connected economy, where more people are online using more devices, and where computing becomes part of everything we do. Unfortunately, with our increasing dependency on the digital world, new threats are added every hour. It is all too clear that, as the world gets smaller, cyber risks keep getting bigger.

To help businesses and public sector entities build secure modern IT infrastructures, we at HP, have been studying the evolution of cyberattacks and threat actors over many years. Our research has led us to invest heavily in research and technical security innovation for endpoint devices in order to ensure we can keep ahead of the degrading threat landscape. And we are not the only ones to observe increasing threats to users' devices. According to a recent survey, in the past six years, the percentage of breaches involving a compromised user's device has more than doubled, whereas attacks on servers and networks have declined[1].

With this trend as a starting point for a more in-depth analysis, this article explores ways in which endpoint security becomes more and more significant in the era of the 'Internet of all things'. We focus in particular on the most common types of attacks and the reasons why businesses and governments should consider device security a top priority area for investment. We conclude with some recommendations for a cyber-resilient approach to risks.

Connected endpoint devices in the office: where are attackers going to hit most frequently?

There is a lot of noise around the Internet of Things, but we are still rather far from a scenario in which our own

1 | Verizon, 2016 Data Breach Investigations Report, 2016.

shower is at risk of being a vector of hacking. However, if we concentrate on businesses and the public sector, and think about an average office, the risk is very real: anything with connectivity has the potential of being an attack vector and lead to compromising data privacy and confidentiality.

Dealing with threats in this kind of environment means taking into account ALL end-user connected devices. In the office this does not just mean PCs and or mobile phones, but also printers and any other embedded devices in the productivity area.

> “ Only 53% of IT managers realise printers are vulnerable to cybercrime. Deeper integration of printers into enterprise networks and smarter functionality mean that they look a whole lot like PCs, and are, by all standards, an IoT device.

PCs remain one of the most common and most often targeted devices. Still, at least 400 million PCs are more than 4 years old in offices around the world, which typically denotes they use outdated technology that makes them vulnerable[2]. Mobile phones are in a similar category, with users forgetting to download updates or using their personal phones for work, too. Printers are also typical office equipment, but despite this fact, many Chief Security Officers do not pay attention to printer fleets as much as they should. Only 53% of IT managers realise printers are vulnerable to cybercrime[3]. Deeper integration of printers into enterprise networks and smarter functionality mean that they look a whole lot like PCs, and are, by all standards, an IoT device.

Printers share many of the same hardware capabilities as PCs, including powerful processors, disk drives, and users interfaces. This is true of firmware and software alike: printers have BIOS firmware and built-in operating systems; they run application executables and use common network protocols. Today’s printer is a fully functioning endpoint device on a network. From the point of view of cybersecurity, printers require the same degree of protection as PCs, and recent attacks conducted through printers confirm the need to take that very seriously[4].

Other devices are slowly integrating into our smart office, such as smart air conditioning[5], smart TVs, and other connected devices. And the more useful these connected devices are, the more we should pay attention to how we can maintain good cybersecurity practices and protection mechanisms around them. Those same innovative functionalities that make our connected devices attractive should prompt businesses to consider where things could go wrong.

Attacks on the endpoint firmware with far-reaching consequences: complete control and stealth

Cybersecurity breaches come in many different forms. In terms of attacks targeting endpoint devices, malware (malicious software) is today’s most common method[6], spreading through multiple mechanisms and actively hiding from security systems. Amongst different types of

2 |with outdated security in the operating system, with no BIOS protection from persistent and stealthy malware, exposed to visual hacking, with no policy enforcement, and weak password protection.

3 | Ponemon Institute, “Annual Global IT Security Benchmark Tracking Study”, March 2015, sponsored by HP.

4 | Printers in several American universities were made to print anti-Semitic fliers in a hack. See for instance Jen Wieczner “This Hacker Sent Nazi Flyers to Thousands of Printers In Internet of Things ‘Experiment”, Fortune 2016 http://fortune.com/2016/03/29/hack-printers-internet-of-things/ (access: 14.03.2017).

5 | Which has already been shown to be a perfect attack entry point. See for instance Kim Zetter, “How to Hack the Power Grid Through Home Air Conditioners”, Wired 2016 https://www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/ (access: 14.03.2017).

6 | Lloyds, “Managing digital risk: Trends, issues and implications for business” https://www.lloyds.com/~/media/lloyds/reports/360/360%20digital/lloyds_360_digital_risk_report%20(2).pdf (access: 14.03.2017).

malware, the type of malicious software that attacks end-point devices at the firmware level is often overlooked.

Firmware, which includes the system BIOS in Personal Computers or printers, is, in a nutshell, the lowest level of embedded software that is required to keep the hardware working. It is responsible for allowing hardware devices to communicate with each other, and for the operating system to be able to run on a device.

Firmware exists not only in PCs and printers, but in all embedded devices, be they smart washing machines, or cars. The 2016 Intel McAfee Labs Threat Prediction Report[7] highlights firmware attacks as a fast-growing area. Their numbers and reach are predicted to increase over the next five years. These attacks targeting firmware below the device's Operating System (OS) are among the ones that are most likely to grow not only in number, but also in seriousness – for various reasons. The return on investment on a firmware level attack is high for attackers because it gives them the deepest level of control on a device. It is virtually non-detectable on a traditional piece of equipment that was not designed with firmware cyber-resilience in mind, and cannot be removed without a major maintenance intervention. On top of all this, firmware attacks open a path for attackers to disable hardware completely, and at the lowest level, gain a foothold into a device to mount further destructive attacks.

Firmware attacks are troubling for a number of reasons. Residing in a non-volatile memory on a device's circuit board, firmware is typically the first code to execute on a device when it is turned on. It configures the device's hardware and sets controls over access to hardware resources in the OS or application platform code. In PCs, this includes specific firmware-controlled features (such as pre-boot authentication), and the enabling and disabling of different functionalities (such as booting a USB connected drive or even disabling some network interfaces altogether). After firmware has finished booting, OS and application software will run under the assumption that they cannot bypass any controls enforced by firmware.

If an attacker manages to penetrate the device's firmware, they can seize control of most of the device's resources. Importantly, an attack that takes control of the firmware execution environment has access to and control over all hardware resources, including the code and data of all the software stack, OS (or embedded OS), and applications executing on the device[8].

This sounds really complex, but what does an attack to firmware look like? It can resemble any other types of attacks. An employee clicks an email link or opens a PDF, but in effect this seemingly innocuous action triggers a phishing attack targeting BIOS – the PC firmware. In most PCs, BIOS can be compromised and the user may never know. Firmware attacks are almost impossible to detect because firmware is invisible to OS and traditional software security applications. Firewalls or anti-virus cannot scan BIOS or other PC firmware either. Once an attacker has penetrated firmware, they gain the ability to monitor any software operating on a device and inject their own software into the system that essentially provides them a stealth and persistent backdoor into the device. Such attacks can then be used to pursue other traditional attack avenues: to steal credentials and intellectual property, insert ransomware to blackmail a user into parting with money or data, and even block hardware operation and disable the device completely and permanently. And given that this type of malware (often known as a firmware rootkit) can escape all client device software security solutions, it can be persistent and impossible to remove without a system board replacement.

While these kinds of attacks have recently become more sophisticated, they are not entirely new. The notorious CIH Chernobyl virus appeared as early as 1999,

7 | Intel McAfee Labs, "Threat Prediction Report", 2016, p.9 https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf (access: 14.03.2017).

8 | Kim Zetter, "Hacking BIOS Chips Isn't Just the NSA's Domain Anymore", Wired 2015 http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/ (access: 14.03.2017).

erasing PC firmware on the system board and rendering the system totally inoperable, which required a system board replacement to recover. Today there is more and more evidence of commercialised firmware rootkits, such as Mebromi[9] or the PC firmware rootkit malware that the Hacking Team was caught selling in summer 2015[10].

Ensuring devices are cyber-resilient is the key to a safer cyber-physical world

Considering how fast we become more connected by using more devices, it is urgent for companies and governments to assess not only how to limit damages from traditional software attack vectors, but also to take into account firmware attack risks. We at HP believe that a key principle beyond any strategy against cyberattacks is cyber-resilience. As Simon Shiu, Director of HP Labs Security Lab, reminds us system security architecture design should now be as much about resilience and recovery as simple defence. It's a more nuanced approach that accepts the inevitability of data breaches but not their capacity to cause serious business disruption[11].

Cyber-resilience starts with good initial protection. Such safeguards must constantly be increased as the threat landscape degrades. This makes many industry security best practices essential, from designing security architecture for firmware integrity protection to ensuring that security settings are properly configured before a user gets their hands on a device. For example, the 'security by default', or 'security by design' approaches are important for manufacturers to ensure that they take security into account from the very earliest stages of design and configuration of a device. Governments Cyber Security strategies around Europe[12] are slowly starting to adopt this as a key principle. It should become a cornerstone of their procurement patterns, and it should be applied more widely by businesses, too.

However, protection is not enough in order to achieve cyber-resilience. It becomes essential to design detection mechanisms from the ground up and incorporate them into the very device architecture to ensure that when protections are successfully bypassed, the attack can be detected. This is particularly important to allow appropriate remediation steps to be taken, given that older devices are incapable of detecting successful firmware attacks.

Finally, cyber-resilience can be achieved when recovery to a good state can happen swiftly and efficiently once an attack has been detected. While recovery may look different depending on the environment and customer needs, the aim should be to ensure minimal productivity loss and the ability to quickly recover to a good working state in case of an attack.

An example of how HP has applied the principles of design for cyber-resilience to its own products is HP Sure Start[13]. This state-of-the-art device security capability delivers a self-healing firmware solution in HP business PCs and printers. By using an independent chip capable of detecting firmware intrusion into PC BIOS and printer firmware, HP Sure Start is able to report and repair it instantly, and can even be automated with policy controls by a user or administrator. HP Sure Start validates the integrity of the firmware image before it is executed at boot. If validation fails, a protected and cryptographically verified 'Golden Copy' of the firmware is used to repair the device. The Golden Copy is stored in a private, isolated Non-Volatile Memory (NVM) that no third party firmware or software can access.

9 | Livian Ge, "BIOS Threat is Showing up Again!", Symantec 2011 http://www.symantec.com/connect/blogs/bios-threat-showing-again (access: 14.03.2017) and Marco Giuliani, "Mebromi: the first BIOS rootkit in the wild", Webroot 2011 https://www.webroot.com/blog/2011/09/13/mebromi-the-first-bios-rootkit-in-the-wild/ (access: 14.03.2017).

10 | "Hacking Team spyware rootkit: Even a new HARD DRIVE wouldn't get rid of it", The Register 2015 http://www.theregister.co.uk/2015/07/14/hacking_team_stealth_rootkit/ (access: 14.03.2017).

11 | Simon Shiu, quoted in: "Why resilience is the future of cyber security", The Telegraph 2017 http://www.telegraph.co.uk/business/sme-home/hp-resilience-and-cyber-security/ (access: 14.03.2017).

12 | E.g. in the UK https://www.ncsc.gov.uk/articles/secure-default and in the Netherlands https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html (access: 14.03.2017).

13 | HP Sure Start Gen 3 Technical White Paper 2017 http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA6-9339ENW.pdf (access: 14.03.2017).

Conclusion: reaching the endpoint of end-point security?

We move towards a world where more and more devices are connected. A growing number of these devices are deployed without applying well-established IT security best practices. Worse yet, many of them are not designed to survive modern cyber threats. This results in numerous new products reaching the market with all too manifest vulnerabilities. A device with poor security design or poor security management can open a whole network up to an attack, giving malicious actors access to a larger attack surface than ever before.

The need to secure devices becomes critical as the majority of attacks are launched at the end-points. And the device security should be approached from the bottom up, starting from firmware. As explained in this article, firmware rootkits are particularly insidious because of their stealth and persistency. Today's decision-makers, both in private companies and public organisations, should prioritise device security and put it at the forefront of their battle for cybersecurity.

In the future, consumers and businesses should be able to trust their devices, and see them as an opportunity rather than a threat. Therefore, security solutions are, and should be, absolutely central for key future technology disruptions such as 3D printing, the digitization of manufacturing, and the emerging cyber-physical world around us. ■

CYBERSEC 2016
IN NUMBERS

1
Emerging Public Policy Challenge

2
Days of Thought Provoking Debates

4
Thematic Streams

>400
Articles about CYBERSEC

40
Accredited Journalists

35
Interviews for CYBERSEC TV

79K
Twitter Impressions

20
Hours of Networking Opportunities

>120
Speakers

10%
Academy & NGO

30%
Public Administration

50%
Private Sector

10%
Military & Police

LEARN MORE ABOUT @CYBERSECEU:

INTERVIEW WITH SZYMON KOWALCZYK

SZYMON KOWALCZYK
Group Chief Information Officer/Executive Directorat TAURON Polska EnergiaS.A. A graduate fromtheTechnical University of Legnicain computer systems and networks, Mr Kowalczykhas worked in information technology for 23 years. Hehas extensive experience in fusion projects, system and infrastructure consolidation as well as process and IT cost optimization. In 2007, his platform consolidation through virtualisation project received the first prize in the category "Infrastructure Simplification" in an international competition held by Common Europe. In 2009, he won the competition organisedby HDI Poland in the category "Venture of the Year 2008"for implementing the project "Business optimization and improvement through IT servicesconsolidation". In the years 2010-2012,he was the Director of the"Annapurna Scheme"aimed to establisha modern bank based on mobile solutions,harnessingthe potential of the sales and technology network of one of the leadingmobile phone operators in Poland. From 2012 to2013,he executeda projectthataimed to reorganise and consolidate ITunitsin order to increaseoverallefficiency and optimize processes during change implementation, while ensuring HA parameters ofIT services.

Tauron Group is one of the largest energy holding companies in this part of Europe. Different studies show that the energy sector is particularly vulnerable to attacks carried out in cyberspace. What cyberattack vectors do you most frequently detect? Which ones would you consider the most dangerous?

The attack vector that we most commonly observe targets our employees. It includes both emails and infected USB flash drives, or malicious content on Web pages. We have noticed that these attacks are becoming increasingly better prepared, which makes the messages harder to diagnose as malicious. Similarly to other sectors, we also detect attacks on our Internet-connected infrastructure.

In his book Blackout, Marc Elsberg depicts a catastrophic cyberattack which on one winter morning causes a power outage in Europe. Is the scenario pure science fiction or reality that we should be concerned about here in Europe?

As Ukraine's experience has demonstrated, the Blackout scenario is by all means possible, but probably not to the extent that Marc Elsberg describes. We are aware of how critical the continuity of production and power supply is for the functioning of the state. Therefore, we track cybersecurity trends as well as the emerging new threats in order to best protect our ICT and industrial automation infrastructures.

In Poland we expect legal changes to happen that will strengthen cybersecurity, among other things, the drafting and passing of the Cybersecurity Act. What does a company like Tauron, which is actively involved in initiatives that improve cybersecurity, expect from the Act? What elements should it contain to genuinely enhance the country's ICT security?

It is necessary to regulate the rules of cooperation and the exchange of information about threats. As past

experience shows, cyberattacks are rarely mounted on the entire industry; more often they target one or several companies at a time. Then, slightly modified, they hit other entities a few days later. By knowing more about the situation in cyberspace than we do today, we can respond better and faster to incidents.

We are aware that various entities increasingly highlight the problem of a shortage of cybersecurity specialists. What does this look like from your point of view? Is this actually a real problem? We know that your company teams up with universities, but do these partnerships in any way address the need for more cybersecurity specialist?

TAURON group is taking action to ensure that there is the best possible match between the knowledge and skills that graduates acquire and the tasks they will potentially perform as the employees of TAURON group. However, we also see the need for a systemic solution to effectively address challenges in cybersecurity education. We believe security-related modules should be integral to study courses educating future IT professionals or automation engineers.

How do you assess the cross-sectoral cooperation that aims to share efforts in order to strengthen cybersecurity?

The cross-sectoral cooperation has a short history, so it is not too far advanced yet. Nevertheless, we all realize that we need to work together to become more resilient to cyberattacks. Therefore, we engage in various activities, share our experiences and knowledge. We also meet on a regular basis and talk about the biggest cybersecurity challenges.

Can the state, the public administration that is, support your cybersecurity efforts in any way?

The state can help by disseminating knowledge about cyberthreats. A dozen or so years ago, no one was teaching computer science in schools. Today it is a subject like many others. Cybersecurity should follow the same path. Another important aspect is to start certifying ICT solutions for safety. These projects are expensive, but their outcomes would allow us to build more secure infrastructures. ■

ANALYSIS

CYBER-ATTACKS AND THE NATO ALLIANCE ARTICLE 5 MUTUAL DEFENSE CLAUSE: THE EFFECT ON PRIVATE SECTOR CYBERSECURITY STRATEGY AND INCIDENT RESPONSE

ADAM PALMER
Adam Palmer (MBA, JD, CISSP, CIPP) is a former U.S. Navy Officer, Prosecutor, and former Manager of the U.N. Global Programme Against Cybercrime. He is a Senior Research Fellow of the Kosciuszko Institute, Adjunct Cybersecurity Advisor for the Singapore RSIS policy group, and Vice President of Cybersecurity Risk Management for the Financial Services Roundtable.

NATO Secretary General Jens Stoltenberg stated in June 2017 that the Article 5 Mutual Defense Clause of NATO may be activated in response to the recent cyber-attacks experienced across Europe[1]. "The attack in May and this week [June 2017] just underlines the importance of strengthening our cyber defenses and that is what we are doing," Mr. Stoltenberg cautioned. The possible activation of Article 5, for the first time since the September 11 World Trade Center attacks, highlights the recognition of cyberspace as new global "war-fighting" domain on equal footing to traditional threat landscapes of sea, air, and land[2].

Cyber threats are increasingly shifting from a law enforcement domain to a militarized nation-state focused threat landscape. Cyberspace is a unique domain in which the lines between civilian and military targets are blurred and the warfighting domain is itself built upon civilian networks. Militarization of cyberspace is dramatically affecting the overall approach to cybersecurity strategy across both industry and government. It is now critical

1 | See, http://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples.

2 | Id.

for multi-national corporations to understand when and how a military response might be relevant (or mandated) to a cyber incident. It is critical to understand how military operations may play a direct role in protecting civilian cyber infrastructure thru an active defense capability in the same manner as the traditional domains of sea, air, and land. And it is critically important for industry to be involved in the decision-making process for cyber response, or at least alerted, when a response may escalate attacks or draw additional actions that impact the target industry.

This is a complex issue involving international and operational law, however, for purposes of this article, the focus will be on understanding the impact of transnational cyber-attacks on the NATO Article 5 mutual defense clause. The role of NATO in cyberspace will impact cybersecurity strategy, public-private partnership, and incident response for both government and private sector.

Nation-State Military Response to Cyber-Attacks

Echoing the comments of NATO, Michael Fallon, the British Defense Secretary, recently stated that the UK might consider retaliating with unilateral military means against a cyber-attack by another state[3]. The likelihood of military response is particularly compelling in scenarios such as the June 2017 cyber-attacks in Ukraine. Experts believe these recent attacks used an exploit similar to last May 2017's "WannaCry" ransomware attack, however, unlike WannaCry, the latest attack appears designed to cause network destruction rather than to extort money[4]. "The money-gathering element was amateurish and not in line with what we expect from professional cyber criminals. . . that suggests the motivations are actually either a deliberate attempt or experimental attempt to create disruption, operational disruption, to larger government and corporate organizations," stated Brian Lord, a former deputy director of intelligence at UK intelligence agency GCHQ[5]. Almost all Ukrainian government departments, the central bank, a state-run aircraft manufacturer,

> "Cyberspace is a unique domain in which the lines between civilian and military targets are blurred and the warfighting domain is itself built upon civilian networks.

the Chernobyl nuclear plant, and Kiev's main airport and metro network were all temporarily paralyzed[6].

NATO Recognition of a Cyber Warfare Domain

The NATO alliance first considered cyberspace as a new warfighting domain at the 2002 NATO Summit in Prague with NATO leaders expressing additional support for protecting global information systems 4 years later at the 2006 NATO summit in Latvia. NATO discussion on cyberspace increased greatly following the cyber-attacks against Estonia in 2007 and NATO released its first public policy on cyber defense in 2008. Following the NATO cyber policy declaration, a conventional military conflict, preceded by cyber-attacks, occurred between Russia and Georgia in the summer of 2008. Witnessing cyber-attacks being incorporated into conventional battle strategy led NATO to further accelerate its approach to cyberspace by creating a goal in 2010 to develop an in-depth cyber defense implementation plan. This was followed in 2012 by the first major step of creating the new NATO Communications and Information Agency (NCI). In May 2014, the NCI achieved full operational capability.

During this similar time-period, NATO also developed the NATO Industry Cyber Partnership (NICP) to improve public-private partnership. NATO and the EU also formed an agreement with the Computer Emergency Response Team for the EU (CERT-EU) to exchange information and best practices for cyber defense.

3 | Id.
4 | Id.
5 | Id.
6 | Id.

On June 14, 2016, NATO formally recognized cyber-space as a war fighting domain at the NATO Warsaw Summit. Like all conventional domains (air, sea, land), NATO 's mission in cyberspace is defined as defensive only. During the Warsaw Summit, NATO members also pledged to improve cyber defense of their national critical infrastructure and national telecommunications networks.

Finally, in early 2017, NATO adopted an updated cyber defense plan and implemented a new road map to implementation of cyber defense strategy. Current NATO alliance cybersecurity policy reflects member state recognition of the need for improved cyber defense governance, mutual assistance procedures, and the integration of cyber defense into private sector operational strategy planning. A key component of this strategy is increasing NATO's cooperation with industry on information-sharing and the exchange of security best practices. NATO's cyber defense policy includes goals for additional capability development, education, training, and industry partnerships[7].

NATO Cybersecurity Policy Framework

NATO policy on Cybersecurity is implemented by NATO's political, military and technical authorities and individual Allies. The North Atlantic Council (NAC), within NATO, provides high-level political oversight. The NATO Cyber Defense Committee, subordinate to the NAC, is the lead committee for political governance and cyber defense policy. The NATO Cyber Defense Management Board (CDMB) is also responsible for coordinating cyber defense at the operational level. The NATO Consultation, Control and Command (NC3) Board is the main committee for consultation on technical and implementation issues. The NATO Military Authorities (NMA) and NCIA are responsible for operational requirements, acquisition, implementation, and operating of NATO's cyber defense capabilities.

7 | See www.nato.int/cps/cn/natohq/topics_110496.htm.

Public-Private Partnership: Solving the "David vs. Goliath" Security Challenge?

The cyber version of "David vs. Goliath", giant vs. small target, challenge is the small private sector commercial IT department forced to defend against weapons grade state-sponsored cyber-attacks. This was highlighted in the widely publicized "APT 1 report" produced by Mandiant Corporation in which specific Chinese military operatives (Advanced Persistent Threat Group 1) were identified and linked directly with attacks against commercial businesses[8]. While increased militarization of cyberspace may exacerbate the imbalance of adversary power, the addition of NATO member cyber resource capabilities may also be a source of additional support to equalize capabilities. This may be particularly useful in using "active defense" techniques such as defensive worms or intelligence gathering. These, and a variety of other so called "hack-back" techniques, are properly placed solely within a government context where authorities have greater access to classified information to identify attackers or conduct advanced intelligence gathering operations to determine attribution.

> "To promote a common approach to industry partnership for cyber defense capacity building, NATO has established implementation guidelines.

Cyber-attacks have rapidly increased in frequency and complexity during the last decade. Ransomware attacks, advanced persistent threats, distributed denial of service attacks, phishing, malware, and botnet armies comprised of Internet-connected devices (the "Internet of things") present a disturbing array of threats to critical infrastructure. There is scarcely an institution of government,

8 | See https://www.fireeye.com/content/dam/fireeye-www/.../mandiant-apt1-report.pdf.

banking, financial, or insurance services that has not been the victim of a data breach or attack.

To promote a common approach to industry partnership for cyber defense capacity building, NATO has established implementation guidelines. This includes integrated cybersecurity planning into NATO's Smart Defense initiatives. Smart Defense is a NATO program that enables countries to work together to develop and maintain advanced capabilities. Cyber Smart Defense projects include the Malware Information Sharing Platform (MISP), the Smart Defense Multinational Cyber Defense Capability Development project, and the Multinational Cyber Defense Education and Training program. Through the NATO Industry Cyber Partnership (NICP), NATO is also working to reinforce its relationships with industry. This partnership utilizes existing frameworks (Computer Emergency Response Teams (CERTs) and others) and manages Information-sharing, training, and education projects with the private sector.

A NATO Article 5 Triggering Event in Cyberspace

"A state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects"[9]. The right to national defense has been clearly recognized to extend beyond kinetic armed attacks to asymmetric cyber operations and some cyber operations may be sufficiently serious to be classified as an "armed attack" within the definition of the United Nations Member charter[10]. A series of low threshold attacks may also collectively rise to the level of a triggering "armed attack" if viewed as a composite attack[11]. In considering the level of harm that may be considered in terms of "scale and effect", all reasonably foreseeably consequences of a cyber-attacks should be considered in determining its scope and severity for purposes of determining justification for NATO self-defense actions[12].

"A series of low threshold attacks may also collectively rise to the level of a triggering "armed attack" if viewed as a composite attack.

It is generally accepted that the International Law Commissions Articles on State Responsibility, recommended by the UN General Assembly for member state adoption are applicable to the issue of nation state responsibility in cyberspace[13]. In the Tallinn Manual 2.0, the recently revised and widely accepted reference guide for international law applicable to cyber operations, a nation state is defined to be responsible for a "cyber related act" if such an action constitutes a breach of an "international obligation"[14]. An international obligation is more than an economically harmful or unfriendly action. The International Court of Justice has stated that a breach of an "international obligation" may only occur by an intentional act or also an omission to act as legally obligated under international law[15]. The term "cyber related acts" is also utilized to encompass acts that may indirectly facilitate cyber-attacks such as a nation state making its networks available to attackers to utilize them, failing to take reasonable efforts to terminate cyber-attacks using national networks, or providing technical support to attackers[16].

Beyond direct attacks from state actor, a critical issue for cybersecurity incident response is the handling of a non-state actor engaged in corporate espionage in cyberspace by utilizing tools or technical support from a national government. The cyber-attack of a non-state actor is attributable to a state actor if a state "factually exercises 'effective control' over the conduct of the non-state actor"[17]. The burden of proof for determining 'effective control' of a non-state actor's activity is

9 | The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p.339.
10 | Id, p.340.
11 | Id, p.342.
12 | Id, p.343.
13 | Id, pp.79-80.
14 | Id, p.84.
15 | Id.
16 | Id.
17 | Id, p.81.

variable depending on facts and jurisdiction. There is no generally accepted duty that evidence of attribution must be publicly disclosed prior to taking actions in response to an attack in cyberspace[18].

The right of "Collective Self Defense" against cyber threats has been specifically recognized by both the international authors of the Tallinn Manual and pursuant to the collective defense rights outlined in UN Charter Article 51[19]. A NATO member state may participate in collective defense against cyber threats pursuant to Article 5, provided that, the member state adheres to international principles of proportional response, imminence, necessity and immediacy applicable to collective defense[20].

Cyber-Attacks Against Non-NATO Member Nations

As the most capable global military alliance, NATO carries weight in international cybersecurity affairs. NATO may facilitate cyber threat information-sharing, even among non-NATO member states. NATO cooperation also offers a route to cooperate with the United States for common strategic objectives. This is particularly critical in cases where a non-NATO member-state hosts multi-national industry assets that play a critical role in the global commercial network. Cyber-attacks against these critical assets may pose not only a risk to the nation-state, but a systemic risk to global markets.

In Eastern Europe, the type of multilateral security cooperation required to effectively respond to interconnected, trans-national, cyber threats is still immature. Cooperation with NATO – participating in NATO's exercises and training – provides an opportunity for partner countries in smaller Eastern European nations to become familiar with multilateral approaches to cybersecurity planning and response operations. This offers increased opportunities for closer multi-national cyber incident response cooperation.

18 | Id, p.83.
19 | Id, p.354.
20 | Id, p.355.

It is important that public-private cooperation be accelerated to address the potential systemic risk that cyber threats present. An adversary might attack a multi-national industry regional office rather than a more hardened target in the home NATO country. The 2013 cyber-attack against Target Corporation also highlights the concern about attack escalation. The devastating attack against Target originated thru an HVAC vendor. The attacker used this weakness to escalate a widespread attack against the entire enterprise. This strategy could be adopted by an adversary attacking foreign based operations. The strategy would be to penetrate a regional office and escalate across networks to a global headquarters.

"In Eastern Europe, the type of multilateral security cooperation required to effectively respond to interconnected, trans-national, cyber threats is still immature.

Attacking a major multi-national office in Eastern Europe also could risk systemic catastrophic harm by disabling the communications network between the regional office and its headquarters offices in the EU or US. Such an attack, outside the land borders of NATO members, would still potentially cause severe damage to NATO member economies and possibly trigger an Article 5 mutual defense response.

Finally, it is critically important for private industry to be involved in the decision-making process for cyber response, or at least alerted, when a response may draw additional attacks. A nation state response to a cyber-attack may further impact private industry. For this reason, industry should be alerted to government activity that may increase risks of counter attacks. Government should create support programs to defend against such counter-attacks so that industry does not solely bear the costly burden of being in the "cross-fire" of nation state cyber warfare.

Conclusion

As NATO considers the events that may require a collective defense military response against cyber-attacks, it must also evaluate the level of support provided to defense of commercial networks. It is not practical, or desirable, for NATO or national defense networks to intrude into commercial networks. However, there must be greater attention to developing and harmonizing protocols for cooperation and sharing of threat information. Multi-national commercial enterprises must be able to rely on support from government defense capabilities and intelligence to improve capabilities. This should be done within a context of protecting the privacy and independence of commercial entities and Internet users. Consideration must also be given to the risk that an adversary may target regional offices of multi-national industry in an attempt to disrupt global markets or attack a brand as a symbol of foreign commercial industry. ■

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION OFFER

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 receive the ECJ, please use the online subscription form at www.cybersecforum.eu/en/subscription

Follow the news @ECJournal

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