VOLUME 2 (2016) ▪ ISSUE 3

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

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

ISSN: 2450-21113

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

THE KOSCIUSZKO INSTITUTE

Citations: This journal should be cited as follows: "European Cybersecurity Journal", Volume 2 (2016), Issue 3, 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

The fourth issue of the ECJ is published following the North Atlantic Treaty Organization Summit in Warsaw. Undoubtedly, it is yet another Summit on which important decisions, from the NATO's cyber defence policy perspective, were taken. Cyberspace has been recognised, alongside air, sea, land and space, as an operational domain.

Bearing in mind the importance of this decision, in this issue of the ECJ, we mainly focus on further challenges concerning development of NATO's cyber defence policy. In her article, Kate Miller presented a brave analysis calling the public to start a serious debate on the conduct and planning of even bolder actions within the realm of cyberspace.

The consequences deriving from the fact that the cyberspace may be used for military actions are also depicted in Jeff Carr's article which analyses the problem of "Under What Circumstances May Civilian Hackers Be Targeted For Killing." This is a challenge which should not be considered as a future scenario, but as an existing problem which international community must face today.

The fourth issue of the ECJ reflects an innovative analysis of a case study conducted by Exatel which helps us to understand how important it is, from the cybersecurity point of view, to make conscious decisions regarding the use of the Internet on a daily basis. In this particular case, "the main actor" of the analysis is a web browser.

The perspective oriented towards a more strategic thinking is reflected in an article written by Jani Antikainen which highlights, often insufficiently, emphasised aspects of ensuring the integrity of data. Risks associated with the possible "Information Sabotage" could lead to enormous consequences not only at the level of individual entities, but also at the level of states.

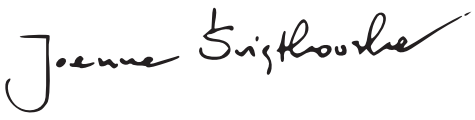
There is also an article written by Jack Whitsitt who, having encountered incorrect approaches towards thinking about the information security, points out the essence of the problem as well as specific recommendations.

This issue of the ECJ contains an analysis of Robert Siudak which, by judging issues of interoperability and the openness of the Internet in a wide context, presents the brand new initiative of the Kosciuszko Institute and our Dutch partners, devoted to the internet standards.

Finally, the fourth issue of the ECJ provides you with two very interesting interviews with Olivier Burgersdijk and Dean Valore, both related to the challenge of combating cybercrime.

Above all, we believe that recommendations from the articles concerning the future of NATO's cyber defence policy will be an important source of inspirations for decision-makers. The conclusions drawn from other articles will definitely also be useful for individual users.

I wish you an inspiring reading.



CONTENTS

5 INTERVIEW WITH OLIVIER BURGERSDIJK
Olivier Burgersdijk

8 PLANNING FOR CYBER IN THE NORTH ATLANTIC TREATY ORGANIZATION
Kate Miller

17 UNDER WHAT CIRCUMSTANCES MAY CIVILIAN HACKERS BE TARGETED FOR KILLING?
Jeffrey Carr

20 INFORMATION SABOTAGE – A CYBER'S UNDISCOVERED COUNTRY?
Jani Antikainen

29 DANGEROUS WEB SURFING – "I WILL BE VERY SURPRISED IF THIS COMES TO LIGHT
SOC Exatel

39 OPEN AND SECURE – THE ROLE OF THE INTERNET STANDARDS IN GOVERNING CYBERSPACE
Robert Siudak

44 INTERVIEW WITH DEAN VALORE
Dean Valore

46 THE TRAP OF INFORMATION SECURITY" & ESCALATING CYBER RISK
Jack Whitsitt

53 TRENDS IN JOINT NATO-EU CYBERDEFENCE CAPABILITIES
Piotr K. Trąbiński

INTERVIEW WITH OLIVIER BURGERSDIJK

OLIVIER BURGERSDIJK
Mr. Burgersdijk, after finishing a university education (Criminology), joined the Rotterdam-Rijnmond police force in The Netherlands (1998-2001). There he was active in the areas of conducting evaluations on major criminal investigations of serious and organised crime as well as strategic analysis. From 2001 to 2006 he supported as a consultant on various regional police forces and prosecution services in The Netherlands in the areas of quality management, evaluation and information management. From 2006 till present he is active within Europol in different functions with responsibilities for information exchange and information management at strategic as well as technical level. Since November 2012, he is Head of Strategy within the European Cybercrime Centre with responsibility for strategic analysis, outreach, forensic expertise, Research & Development, prevention, training & capacity building and internet governance.

The Network and Information Security (NIS) Directive will be definitely an important achievement that will reshape the European cybersecurity landscape. The Directive states: "incidents in cyberspace may be result of criminal activities and Member States should encourage operators of essential services and digital service providers to themselves report incidents of a suspected serious criminal nature to the relevant law enforcement authorities. EC3 should facilitate coordination between competent authorities and law enforcement authorities of different Member States in this matter" – what instruments the EC3 may use to implement this provision?

This provision in the NIS Directive aims to stimulate the reporting of crimes to the competent authorities in the Member States. These competent authorities can then decide whether to share the information with Europol's European Cybercrime Centre (EC3). This does not change anything directly for EC3 other than hopefully an increased reporting and sharing of information on cybercrimes. The tools EC3 already provides are the ability to share information, including in large volumes and for particular types of information, such as for malware analysis. As part of the service Europol offers the possibility to cross-check the information against other data already shared by other countries in order to identify links and potentially linking up to on-going investigative action. In terms of coordination of actions, EC3 provides strategic and tactical analysis to determine priorities and to select the best opportunities for disruption, investigation, prosecution and preventive action. EC3 also supports initiatives at EU-level that look into the development of common taxonomies and standards to facilitate the sharing of information between law enforcement and, for instance, the CERT community.

What in your opinion shall be done to address imbalance in combating cybercrime and building cyber capabilities between EU Member States?

The speed at which cybercrime elements are expanding across crime areas and the continued technological evolution of these crimes pose challenges for all Member States, especially for getting cyber competence distributed across all areas and levels of policing. The strong cross-border dimension of these crimes in the sense that the same crimes are replicated and committed in multiple jurisdictions make that the joint investigation and prosecution of a criminal network has effects in several affected countries. The current joint approach in which the strongest countries take care of the heavy-lifting has a relieving effect on those countries that are struggling more to get their cyber capabilities up to par with the threat. The Joint Cybercrime Action Taskforce – J-CAT – is an important connector facilitating this joint law enforcement focus on the biggest cyberthreats affecting most countries. It is attached to EC3 as the investigative branch in which cyber liaisons of key EU Member States and several non-EU partners ensure the connection with the cybercrime divisions of the participating countries and agencies. In close co-operation with the EU Commission, CEPOL, Eurojust and the European Cybercrime Training and Education Group, EC3 is also actively involved

in the development of a standardised Training Governance Model for law enforcement at the EU level. As a concrete deliverable, the first version of the Training Competency Framework, which lists the required skills and expertise of the main roles in law enforcement involved in combatting cybercrime, was published at the end of 2014. The framework is currently being revised.

Last year, Europol launched EC3 Academic Advisory Network (EC3AAN). The multi-disciplinary academic network which focuses on forward-looking cyber research and advising on key cybersocietal issues. What, in your opinion, in upcoming years, will be the biggest challenge for law enforcement authorities in combating cybercrime?

The continued increase of legitimate encryption and anonymisation techniques make it more and more difficult to obtain lawful access to the content of data to investigate crimes. The judicial authority in cases of suspicion that serious forms of cybercrime have been committed, may provide for the seizure of computers, servers and mobile devices, and for the lawful interception of the internet traffic and communication, but that no longer gives police officers access to the content for investigative and evidential purposes. Moreover, the growing level of sophistication of the encryption, anonymisation and obfuscation makes any attempts for gaining access more difficult. This includes also the criminal abuse of digital currencies such as Bitcoin. The balance between protecting the privacy of citizens and securing their data versus the need to investigate and prosecute when crimes have been committed is very delicate, but important to foster in the years ahead.

Project 2020 Scenarios for the Future of Cybercrime predicts that expansion in the use of unmanned vehicles, robotic devices and automation will raise the issue of whether computers are intelligent agents. What would be the consequences; could it be a turning point for law enforcement?

It is probably difficult to indicate an exact turning point and the definition of so-called "intelligent agents" in the context of artificial intelligence which may not necessarily be helpful for resolving the issue. What we already see is the connection of a sheer endless list of "smart" devices to the Internet. Some of these are merely there to send information, while others will let external factors influence their own performance. The latter will be most vulnerable for malicious manipulation.

Probably the most risky category to consider in this context is the one of vehicles. The latest types are often connected to the Internet for varying purposes and services. Some of these also have an automated form of driving. Most often for parking, but some can also take part in traffic to get from one location to another in varying forms of autonomy. The worrying part for cars is that the policy level is hardly taking any stance here. We have seen several areas in everyday life in which security considerations have called for strong policy intervention. This applies to the prohibition of trucks transporting chemical substances to use certain tunnels; this applies to strict fire prevention measures in hotels, offices and factories, but when it comes to the interconnection of semi-self-driving cars to the Internet, the preventive voice of policymakers is still fairly weak and undecided.
A very basic example would relate to the question how law enforcement can stop a self-driving car.

As we highlighted in the 2015 Internet Organised Crime Threat Assessment report, the increasing adoption of such smart devices combined with autonomous capabilities and AI-like behaviour will raise the number of legal and investigative challenges, particularly in relation to the criminal abuse of such systems. However, developments in this area will most likely also offer new opportunities for law enforcement to combat criminal activity.

Besides the aforementioned, what do you think are the most alarming cyberthreats? What kind of cybercrimes are at the moment the most fatal?

The most alarming cyberthreats are at present not yet the most lethal ones. Important threats include banking malware, ransomware, both propelled by the crime-as-a-service model, online trade in illicit commodities and services, online grooming of minors and live streaming of child abuse. In the direction of lethal threats one can think of threatening hospitals to hack their computer systems. Although this is becoming an increasing practice, this has not yet led to concrete casualties. In fact, the most frequent deaths related to cybercrime are probably suicides by victims of cyber bullying, (sexual) extortion and data breaches. The figures cannot be determined with certainty because the link with the internet communication cannot always be established.

How to fight these threats?

Where the suicides are concerned, a strong focus on psychology is required. Probably the raising of awareness and reference to hotlines and help services is advised most. Development of prevention and awareness material with content and formats that are most suited for the most probable target audiences can help to get the message(s) across. For the more impersonal types of cybercrime, the combination of enhancing protection and the investigation of crimes should be continued.

Through our work with academia, we also try to gain a better understanding of pathways into cybercrime, i.e. to understand what makes you a criminal and what makes you a victim online. We believe that this will improve our ability to offer better protection and prevention for potential victims online.

How does the EC3 organise its work on countering the global organised criminal groups with countries outside the EU?

EC3 works closely with many partners across the world. Key countries and agencies, such as the US FBI, the US Secret Service, Australia, Colombia and Canada are part of the J-CAT that was mentioned earlier as the central operational instrument for the common fight against the major international cybercrime threats. Furthermore, Europol actively engages also with other operational and strategic partners in various ways. This can be by aligning priorities and, where possible, to co-operate in operational matters. Interpol is among these partners enabling a global law enforcement reach across all regions.

Do you think that countries with lower levels of cybersecurity could become "no go" areas and havens for cybercriminals?

It is maybe not a lower level of cybersecurity that is of relevance in this respect, but rather the level of cyber competence that would make the difference. This notion of cyber competence contains several elements. An important one is legislation, having a legal framework in place that enables the effective investigation and prosecution of crimes. For cybercrime, in particular, such a legal framework includes also partnerships with other countries for the exchange of information and the extradition of suspects. A second element is to have the technical and operational capabilities to effectively investigate and prosecute cybercrimes. This includes the technical skills and competences, as well as the numbers of staff and other resources to deal with the size of the problem. The third element is the protective component to defend the national infrastructure and ecosystems against cybercrime. This part is, in particular, of relevance if there is something to gain for cyber criminals and is only to a lesser extent of influence to becoming a "safe haven" for cybercrime.

Thank you for this comprehensive interview. ■

Questions by:
Magdalena Szwiec
The Kosciuszko Institute

ANALYSIS

PLANNING FOR CYBER IN THE NORTH ATLANTIC TREATY ORGANIZATION

KATE MILLER
Kate Miller is a research and project assistant with the Cyber Security Project at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Previously she has worked with the Center's Project on Managing the Atom and interned with the U.S. State Department, contributing to reporting on European affairs. Kate received her M.A. in International Security and her B.A. in International Relations and French, with a focus on transatlantic security.

Introduction

Over the course of the past decade the North Atlantic Treaty Organization (NATO) has worked to ensure that its mission of collective defence and cooperative security is as effective in cyberspace as it is in the domains of air, land, sea, and space. It has created several bodies and developed a collection of policies to deal with diverse aspects of cyberdefence. With the anticipated elevation of cyberspace to the fifth operational domain of warfare at the 2016 Warsaw Summit, however, the Alliance needs to consider cyber capabilities and undertake planning for operations – including offensive ones – directed beyond its networks. And it should establish a Cyber Planning Group to do it[1].

> "The Alliance needs to consider cyber capabilities and undertake planning for operations - including offensive ones - directed beyond its networks.

Fortunately, while the issue of cyber operations beyond NATO's own networks is a politically difficult one given the complex mosaic of national, transnational (EU), and international law; the role of national intelligence efforts in certain types of operations; and ever-present disputes over burden-sharing, the Alliance already has invaluable experience in developing policies and procedures for contentious and sensitive tools in the form of the Nuclear Planning Group (NPG). This article will thus proceed as follows: It begins with a brief overview of actions NATO has already taken to address cyberthreats. It will then explore why these, while important, are insufficient for the present and any imaginable future geopolitical threat environment. Next, it will address the history of the NPG, highlighting some parallels with the present situation regarding cyber and drawing out the challenges faced by, and activities and mechanisms of, the NPG. Finally, it will make the case that a group modeled on the NPG can not only significantly enhance the Alliance's posture in cyberspace, but can serve as an invaluable space for fostering entente and reconciling differences on key aspects of cyber policy. It concludes that the Alliance needs to consider offensive cyber capabilities and planning, and it needs a Cyber Planning Group to do it.

Given NATO's collective defence mandate, a brief note on the use of the terms "defensive" and "offensive" operations and capabilities is appropriate and even necessary. When the term "defensive" is used here, it refers to activities within NATO's own networks, taken either to protect Alliance information systems, enhance resiliency in the event of a breach, or impede and/or remove any unauthorized presence. "Offensive" operations or capabilities cover the range of activities that may take place outside of NATO networks, including dismantling or sinkholing botnets (networks of

1 | The views expressed are the author's own.

computers infected with malware and controlled as a group), distributed denial of service (DDoS) activities, the introduction of malicious code into adversary networks, etc.

Defensive Efforts

The Alliance, as mentioned, has created a number of bodies to address various aspects of defensive capabilities and policies in cyberspace. The NATO Communication and Information Agency (NCIA), for example, provides technical cyber security services throughout NATO, and through the NATO Computer Incident Response Capability (NCIRC) Technical Centre responds to "any cyber aggression against the Alliance[2]". Along with the NATO Military Authorities, it is responsible for identifying operational requirements, acquisition, implementation, and operating of NATO's cyberdefence capabilities. The Alliance also has a Rapid Reaction Team of six civilians, which can be deployed to NATO facilities, operational theatres, or to support an Ally enduring a significant cyberattack[3]. The NATO Consultation, Control and Command (NC3) Board provides consultation on technical and implementation aspects of cyberdefence, while the Cyber Defence Management Board (CDMB), comprised of leaders of the policy, military, and technical bodies in NATO that handle cyberdefence, coordinates cyberdefence throughout NATO civilian and military bodies[4]. At the political level, the Cyber Defence Committee is charged with political governance and cyberdefence policy in general and provides oversight and advice at the expert level. Outside of the NATO Command Structure and NATO Force Structure, the Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, is a research and training facility that offers crucial cyberdefence education, consultation, and research and development.

The Alliance has also developed and endorsed a collection of policies to guide its approach to conflict in or through cyberspace. In late 2007 it adopted the NATO Policy on Cyber Defence that, as stated in the Bucharest Declaration, emphasized NATO's need to protect key information systems, share best practices, and help Allies counter cyberattacks[5]. The Strategic Concept adopted at the 2010 Lisbon Summit tasked the North Atlantic Council with developing an in-depth cyberdefence policy and action plan, mandated the integration of cyberdefence into operational planning processes, and committed to both promote the development of Allies' cyber capabilities and assist individual members on request[6]. The 2011 Cyber Defence Concept, Policy, and Action Plan updated the 2008 policy and called for the Alliance to further develop the "ability to prevent, detect, defend against, and recover from cyberattacks[7]". It also further integrated cyberdefence into existing policy processes by connecting the CDMB efforts with the Defence Policy and Planning Committee[8]. Finally, at the 2014 Wales Summit, NATO endorsed

2 | Healey, J. and Tothova Jordan, K. NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow, 2014, [online] http://www.atlanticcouncil.org/images/publications/NATOs_Cyber_Capabilities.pdf (access: 28.05.2016), p.4.

3 | Men in black – NATO's Cybermen, 24 April 2015, [online] http://www.nato.int/cps/en/natolive/news_118855.htm (access: 21.06.2016).

4 | Cyber Defence, 16 February 2016, [online] http://www.nato.int/cps/en/natohq/topics_78170.htm (access: 08.06.2016).

5 | Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic council in Bucharest on 3 April 2008, (Press Release (2008) 049) [online] http://www.nato.int/cps/en/natolive/official_texts_8443.htm (access: 30.05.2016).

6 | Lisbon Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20 November 2010, (Press Release (2010) 155), [online], http://www.nato.int/cps/en/natolive/official_texts_68828.htm (access: 21.06.2016); Cyber Defence, op cit.

7 | Chicago Summit Declaration Issued by the Heads of State and Government Participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012, (Press Release (2012) 062), [online], http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en (access: 30.05.2016).

8 | Fidler, D., Pregent, R., Vandume, A., NATO, Cyber Defense, and International Law, [in] Articles by Maurer Faculty. Paper 1672, 2013, [online] http://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=2673&context=facpub (access: 08.06.2016).

an Enhanced Cyber Defence Policy, which clarified for the first time that a cyberattack on a member state could be covered by Article 5 (the collective defence clause) of the North Atlantic Treaty.

These organs and bodies all serve vital functions, but they do not go far enough. At present, the Alliance has only limited publicly articulated policy regarding the use of cyber tools to target adversaries' computers and networks in response to either cyber or kinetic/conventional attacks[9].

> "NATO needs to address the lack of policy around how the alliance and member states may use offensive cyber capabilities in both defensive and offensive operations.

While NATO may have a classified policy or doctrine that goes beyond its statement that it "does not pre-judge any response and therefore maintains flexibility in deciding a course of action" in response to a cyber attack, this suggests a vacuum that undermines the credibility of the Alliance's collective defence and common security[10]. NATO needs to address the lack of policy around how the alliance and member states may use offensive cyber capabilities in both defensive and offensive operations. And it requires a body authorized and equipped to develop that truly comprehensive, integrated cyber policy and situate it within the Alliance's broader strategies and objectives.

The Need For Offense

The question of whether and how NATO should undertake cyber operations outside of its own networks, even in defensive, counter-attack scenarios, is not new. The Alliance has a long-standing defensive orientation and has stated on multiple occasions that its top priority is the protection of its networks and the cyberdefence requirements of the national networks upon which it relies[11]. This stance risks becoming a cyber "Maginot line" rather than an effective strategy, however, and many have argued that it must extend its focus[12]. The Atlantic Council's Franklin Kramer et. al., for example, recently called on NATO to "develop doctrine and capabilities to provide for the effective use of cyberspace in a conflict as part of NATO's warfighting capabilities[13]". James Lewis, Senior Fellow at the Center for Strategic and International Studies (CSIS), has noted that some Alliance members already possess offensive cyber capabilities that are "essential for the kinds of combat operations that NATO forces may carry out in the future" and argues the Alliance needs to enunciate how these would be used in support of NATO activities[14]. And Jason Healey, director of the Cyber Statecraft Initiative at the Brent Scowcroft Center on International Security, has repeatedly called on the Alliance to at least consider offensive coordination if it cannot develop its own offensive capabilities[15].

Offensive cyber capabilities serve a number of purposes. They can act as an important force multiplier, especially in asymmetric conflicts. If,

9 | For an exception, see NATO's Rules of Engagement for Computer Network Operations, contained in Series 36 of the MC-362/1 catalogue.

10 | Defending the networks: The NATO Policy on Cyber Defence, 2011 [online] https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf (access: 08.06.2016).

11 | Ibidem.

12 | Fidler, D. et. al, op cit. p. 23.

13 | Kramer, F., Butler, R., and Lotrionte, C., Cyber, Extended Deterrence, and NATO, [in] Atlantic Council: Brent Scowcroft Center on International Security Issue Brief, May 2016, [online] http://www.atlanticcouncil.org/images/publications/Cyber_Extended_Deterrence_and_NATO_web_0526.pdf (access: 03.06.2016), p. 6.

14 | Lewis, J., The Role of Offensive Cyber Operations in NATO's Collective Defence, "The Tallinn Papers" 2015, No. 8, p. 3.

15 | Healey, J., op cit., p. 6.

for example, conflict broke out in the Baltics, NATO or individual Allies' cyber capabilities targeting an adversary's communications, logistics, and sensors could preclude a fait accompli and buy the Alliance precious time to mobilize land, sea, or air forces[16]. This also suggests that in some ways such tools are an extension or evolution of electronic warfare (EW) capabilities, long essential to assuring information superiority and thus NATO's military effectiveness. In the 1950s, NATO promulgated an EW Policy that recognized "the establishment and maintenance of superiority in [EW] is an essential part of modern warfare" and acknowledge that "since all NATO nations and commands will be conducting [EW] operations, it is essential that the coordination and control be exercised at the highest level feasible[17]". As cyber and EW merge and cyber becomes embedded in warfighting, then, a similar policy that outlines responsibilities and national authorities pertaining to cyber operations is needed.

Offensive capabilities also create strategic flexibility, offering an option that falls between talking and bombing. This is particularly important given the hybrid warfare that has taken place in the NATO neighborhood and the low-intensity conflict work that NATO has participated in. While offensive cyber tools can have destructive and disruptive effects, they can also be temporary and/or reversible, and therefore represent an option that certain Allies may view as more palatable or acceptable. Furthermore, not only do adversaries already use offensive cyber capabilities against NATO, but if conflict breaks out they will have vulnerabilities that are best exploited using cyber means. As Matthijs Veenendaal et al. point out in a cyber policy brief for the CCDCOE, if NATO faced an air attack it would not prohibit the use of airpower – limiting itself to air defense systems – in response[18]. For member states to deny the Alliance cyber capabilities, or even the ability to plan for their use by individual Allies, fundamentally undermines NATO's deterrent posture and its credibility among both its own members and its potential adversaries. It also corrodes NATO's ability to prevail as a collective defence entity in a conflict. Finally, while there is no reason a proportional response needs to be symmetric (i.e. confined to the same domain), an enunciated offensive capability and policy on its use would also impact potential adversaries' risk calculations, forcing them to recognize that NATO can respond in kind, as well as kinetically or conventionally[19].

There are, of course, a number of challenges associated with the use of cyber capabilities, especially in a collective manner. As President Toomas Hendrik Ilves of Estonia noted at the June 2016 CyCon, when it comes to cyber, NATO members are in "intelligence agency mode" where they "share as little as possible and only when necessary[20]". This is to some extent understandable: highly targeted cyber tools often rely on intelligence that is both difficult to obtain and inherently impermanent, making national entities reluctant to share information even regarding a particular tool's anticipated effects. Unlike nuclear weapons, which have more or less the same effect no matter where deployed with the only truly important variable being scale, even partial information about the targeting or functionality of a given cyber capability may allow the target to patch a vulnerability or disconnect a particular device, rendering the tool ineffective

16 | Kramer, F., et. al, pp. 8-9.

17 | NATO Electronic Warfare Policy [in] A Report by the Standing Group to the Military Committee on NATO Electronic Warfare Policy, (MC 64), 14 September 1956, [online] http://archives.nato.int/uploads/r/null/1/0/104853/MC_0064_ENG_PDP.pdf (access: 03.06.2016), pp. 2-3.

18 | Veenendaal, M., Kaska, K., and Brangetto, P., Is NATO Ready to Cross the Rubicon on Cyber Defence? "Cyber Policy Brief," June 2016, [online] https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf (access: 21.06.2016).

19 | Lewis, J., op cit. p. 7.

20 | Ilves, T., President Toomas Hendrik Ilves's opening speech at CyCon in Tallinn on June 1, 2016, [online] https://www.president.ee/en/official-duties/speeches/12281-president-toomas-hendrik-ilvess-opening-speech-at-cycon-in-tallinn-on-june-1-2016/index.html (access: 09.06.2016).

or altering its effect. Sharing such information can increase the likelihood it will be leaked and thus result in what is essentially inadvertent unilateral disarmament. Furthermore, intelligence efforts are under the control of national governments and often require enormous amounts of time and effort[21]. Although it is likely that any adversary which attacks NATO is targeted by member states' collection activities, it is an admittedly complicating factor in any Alliance effort to operate effectively outside of its own networks in cyberspace.

> "Once NATO decides it needs to address offensive capabilities, of course, a key issue will be how it develops plans and policies for their use.

An additional issue is the scale and specificity of any given cyber tool (that is, how easily it propagates and limitations on targeting) and the complicated legal environment in which NATO must operate. The Alliance has to navigate a complex web of national, EU, and international law regarding the conduct of military operations and develop policies and strategies that result from and in legal convergence. While there is evidence that software can be highly discriminate and proportionate and its spread controlled, without sufficient preparatory work its effects can be unpredictable and hard to contain. In particular, untargeted entities may be impacted (although, again, if appropriate preparatory effort is made, such entities should not experience deleterious effects even if they are infected with a piece of code or malware). This suggests additional complications for NATO, which must grapple with the risk that certain strategies will reveal or create friction or legal divergence in the Alliance[22].

21 | Lewis, J., op cit., p. 9.

22 | Fidler, D., et. al, op cit. p. 13.

The Nuclear Planning Group Model

Once NATO decides it needs to address offensive capabilities, of course, a key issue will be how it develops plans and policies for their use. This is where the experience of the NPG is illuminating, demonstrating both the limitations such a group will face as well as highlighting reasons to believe in its potential.

The Nuclear Planning Group was established in 1966 in order to address nuclear weapons in the European theater: an issue that inflamed debate from the beginning on how they might be used (and the consequences of their use) – much as offensive cyber capabilities have done[23]. The introduction of theater nuclear weapons under U.S. President Dwight D. Eisenhower's "New Look" strategy stripped non-nuclear allies of operational control of the Alliance's military posture and handed it to the Americans (and, to a lesser extent, the British), who owned the weapons and thus had significant influence over the strategies that governed them[24].

This imbalance induced dissatisfaction and stress in the Alliance that was further aggravated when new weapons were developed or major revisions in strategy (such as the Kennedy Administration's Flexible Response) were proposed. These tensions, in turn, undermined cohesion – and therefore effectiveness and credibility – within the Alliance. The NPG was thus needed not only to address actual force posture and planning issues related to command and control, but to serve the vital political purpose of preserving cohesion. In much the same way, advanced cyber warfighting capabilities are unevenly distributed among allies, and yet just as nuclear weapons were a central element in the Alliance's defensive posture, so these capabilities will be vital in any future conflict. And like theater nuclear weapons before

23 | Buteux, P., The Politics of Nuclear Consultation in NATO 1965-1980, Cambridge, 1983, p. 3.

24 | Ibidem p. 7.

the establishment of the NPG, cyber capabilities lie largely outside the Alliance's institutional framework.

At its inception, only seven states sat on the NPG at any given time: the United States, United Kingdom, Italy, and West Germany were permanently represented while the remaining seats rotated among eligible nations (i.e. those participating in the integrated military structure)[25]. (Today, all NATO members with the exception of France participate in the NPG, irrespective of their possession of nuclear weapons.) Broadly speaking, the group provided a consultative process on nuclear doctrine within NATO. In particular, it focused on three issues of nuclear planning:
(1) how and under what circumstance the Alliance may need to use nuclear weapons;
(2) the question of what objectives might be served by the use of nuclear weapons in the European theater; and
(3) what kinds of consultation should take place in circumstances where the use of nuclear weapons could be contemplated[26]. The NPG also allowed the Alliance to isolate the issues of nuclear planning and doctrine from other matters, protecting it to some extent from being impacted by disagreements over other alliance policies[27].

Significantly, the NPG largely avoided issues of ownership, physical possession, and therefore of direct control of nuclear weapons and decisions regarding their use, which resided in national governments. This was in part a response to earlier efforts to address nuclear sharing, wherein the aggregation of agreement on participation in NATO's nuclear policy and agreement on ownership, force composition, and decision-making formulae actually reinforced the intractability of the sharing issue[28]. Instead, the NPG focused on allied consultation and participation in planning, an approach that was both politically and operationally more feasible for countries controlling the weapons (primarily the United States). While avoiding joint control, this ensured non-nuclear allies could have a role in the procedures by which those possessing nuclear weapons reached decisions concerning them, offering an avenue to constrain their behavior. For the states controlling the weapons, those processes served to reinforce cohesion in the Alliance and allowed them to win support and acceptance for their nuclear policies[29].

The issue of secrecy, mandated on the part of the United States by legislation intended to restrict the spread of nuclear technology, also had a significant impact on the work of the NPG. On the one hand, this legislation, including the Atomic Energy Act, limited the amount of information on nuclear matters the U.S. government could reveal to NATO allies. In particular, the 1958 amendment to the Atomic Energy Act gave the U.S. Congress the power to veto any "atomic cooperation for military purposes with any nation or regional defence organization…[30]". On the other hand, as early as 1954, in response to the development of a Soviet nuclear capability, the United States adjusted its laws in order to supply nuclear information and materials to its NATO Allies in order to reinforce its deterrent and collective defence[31]. Furthermore, by 1961 the United States recognized that in order to get other Allies to understand and accept as doctrine its strategic innovations, it needed to relax its approach to nuclear secrecy. This led the United States to offer much more detailed information than it previously had regarding both technical characteristics of the weapons and relative force levels and strategic concepts[32].
The above considerations offer key insights into

25 | Cyber Defence, op cit.
26 | Buteux, P., op cit. p. 89.
27 | Ibidem, p. 61.
28 | Ibiden, p. 15.
29 | Ibidem, pp. 184-186.
30 | Nieburg, H., Nuclear Secrecy and Foreign Policy, Washington, D.C. 1964, p. 50.
31 | Ibidem, p. 19.
32 | Buteux op cit. p. 21-22.

how a Cyber Planning Group could function. First, issues of secrecy regarding various capabilities, while they will limit what the Group can discuss, need not prevent it from undertaking consequential work. Identifying circumstances when use might be appropriate and developing procedures for consultation regarding that use require only a general sense of their effects, allowing secrecy regarding precise operation. However, the nuclear experience also suggests that key Alliance members can overcome the habit of secrecy if there is sufficient need for information sharing to reduce friction and facilitate consensus building within NATO. Moreover, there is a sense in some segments of the United States that, as former director of the National Security Agency and Central Intelligence Agency General Michael Hayden has stated, information on U.S. cyber policies is "overprotected" and there is a need to "recalibrate what is truly secret[33]". It may be that as cyber becomes increasingly integrated into military operations, the need for cooperation will outweigh the desire for secrecy.

Another useful lesson that may serve to reduce friction at the outset is that Allied or joint control of offensive capabilities – especially those that rely on extensive intelligence efforts – is likely politically impossible and operationally undesirable. That does not negate the value of consultation and an allied approach to planning for their use, however. Developing a collective understanding of how and under what circumstances these capabilities may be deployed by members on behalf of the Alliance, and the possible consequences of that deployment, can enhance its defensive and deterrent posture by expanding its arsenal and lending credibility to threats to utilize it. It is also vital that interested parties understand what tools and resources are and are not available for their defence in order to assure effective planning.

Furthermore, while Allied use of cyber capabilities that can result in significantly destructive outcomes will likely be highly constrained for the foreseeable future, there is no reason the Alliance should not develop doctrine and/or policies regarding the use of activities such as distributed denial of service attacks or dismantling botnets[34]. These are activities regularly deployed against the Alliance and its member states that, in a time of conflict, may be useful to NATO. Just as the NPG discussed the possibility of using theater weapons to slow a conventional invasion, for example, a Cyber Planning Group should examine how limited offensive tools such as denial of service activities or actively hunting and dismantling a botnet can offer a stopgap measure to disrupt an adversary's malicious activity, even if said adversary is not attacking by cyber means. During the 2008 war between Georgia and the Russian Federation, for example, Georgia's efforts to respond to Russian military maneuvers were impeded by widespread denial of service attacks, website defacements, and related activities that impacted the government's ability to communicate with its populace as well as the outside world[35]. Such capabilities would be useful for NATO and/or its member nations in the event of a conflict.

Finally, it is important to appreciate that the establishment of a Cyber Planning Group would constitute a statement of policy in and of itself, regardless of what it may accomplish. Just as creating the NPG signaled to both the Soviet Union and to NATO members that the issue of theater nuclear weapons was a vital one demanding

33 | Hayden, M., Statement of The Honorable Michael V. Hayden, (Testimony), Cyber Threats and National Security, House Select Intelligence Committee, (4 October 2011), [online], http://congressional.proquest.com.ezp-prod1.hul.harvard.edu/congressional/result/congressional/pqpdocumentview?accountid=11311&groupid=103838&pgId=43bc3ae6-fbd2-47a7-b887-914ecc3d3224 (access: 21.06.2016).

34 | This principle has been acknowledge, allowing work to begin on Allied Joint Doctrine for Cyberspace Operations. It is unclear to the author to what extent this doctrine may address activities outside NATO networks, however.

35 | Bumgarner, J., and Borg, S., Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008, 2009 [online] http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf (access: 30.05.2016).

dedicated study by the Alliance, so a Cyber Planning Group could emphasize for Allies and adversaries alike the seriousness with which NATO addresses the issue of comprehensive, integrated cyber operations.

Conclusion

NATO's member states have proven sensitive to discussing cyber capabilities directed beyond its own networks, let alone the question of whether and how the Alliance may use them[36]. Rather than indicating that NATO should let the issue lie, however, the contentious nature of the issue and absence of discussion suggest that consultation and efforts to build consensus are important for alliance cohesion in a volatile and divisive international environment. The fact of the matter is that these capabilities are likely to be crucial in any future conflict. Consultative procedures may serve to reveal and then reduce fractures in the Alliance before those conflicts break out.

The Alliance's central mission of collective defence, including in cyberspace, will soon require a comprehensive cyber operations policy in order to maintain the credibility of both its deterrent and defensive posture. It is an admittedly challenging issue, with many conflicting aspects, but to continue to ignore it will limit NATO's ability to serve as a useful mechanism for handling collective defence, common security, and crisis management. Therefore, NATO should take up the invaluable lessons offered by the experience of the Nuclear Planning Group and either expand the portfolio of the current Cyber Defence Committee (and perhaps the CDMB) to include offensive cyber tools and operations or establish a new body modeled on the NPG.

One of the most remarkable features of the Alliance has been its ability to remain relevant by evolving to address changing threats, ranging from Soviet military power in Europe to international terrorism. By engaging in consultations focused on understanding when offensive cyber capabilities will be most useful and appropriate and what objectives they can help achieve, and developing a coherent yet flexible doctrine, a Cyber Planning Group will assure NATO's continued relevance – and thus its future. ■

36 | Fidler, D., et. al, op cit. p. 24.


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

OPINION

UNDER WHAT CIRCUMSTANCES MAY CIVILIAN HACKERS BE TARGETED FOR KILLING?

JEFFREY CARR
Jeffrey Carr is the author of Inside Cyber Warfare: Mapping the Cyber Underworld (O'Reilly Media, 2009, 2011), the founder of the Suits and Spooks security event, a Senior Analyst at Wikistrat, and the founder and the CEO of Taia Global, Inc. He has consulted for Fortune 500 companies and U.S. and foreign government agencies, and has spoken at hundreds of conferences around the world since 2009. Mr. Carr is widely published and frequently quoted on matters regarding cybersecurity and cyberwarfare in the international mainstream media. He founded Taia Global to assist corporations and government agencies in identifying their high value digital assets and protecting them from theft by competitors, adversaries and insiders.

There are numerous examples of civilian hackers who have conducted attacks against government and civilian targets in times of conflict. Russian hackers supported military operations against Georgia in 2008[1]. Israeli and Palestinian hackers supported their respective nations with cyberattacks during the 2014 war[2].

U.S.-based hackers like "The Jester" have launched cyberattacks against numerous U.S. adversaries like Al Qaeda and ISIS from 2010 up to the present time[3]. The question that this article seeks to answer is when does a civilian hacker who engages in cyberattacks during the times of war become a lawful target like, for example, Junaid Hussain, a British hacker who was targeted and killed in a U.S. military air strike on August 24, 2015[4]. There are three conditions[5] that must be met before the targeted killing of a civilian hacker may occur. If all three of these conditions are met, then the civilian is considered a Direct Participant in Hostilities, which automatically makes him or her a legitimate target.

1. Threshold Of Harm. The act must negatively affect the enemy's military operations or capabilities.

> "There are three conditions that must be met before the targeted killing of a civilian hacker may occur.

1 | Tikk,E. et al, Cyber Attacks Against Georgia: Legal Lessons Identified, NATO CCDCOE, November, 2008, pp.7-8.

2 | Liebelson D., Inside Anonymous' Cyberwar Against The Israeli Government, Mother Jones Online, July 22, 2014: http://www.motherjones.com/politics/2014/07/anonymous-cyberattack-israel-gaza (access: 04.06.2016).

3 | Pagliery J., "Meet The Vigilante Who Hacked Jihadists", CNN Money, January 16, 2015[online] http://money.cnn.com/2015/01/16/technology/security/jester-hacker-vigilante/ (access: 04.06. 2016).

4 | AFP, Jihadist Hacker Killed In U.S. Air Strike Was Recruiter: Pentagon, August 28, 2015 [online] http://news.yahoo.com/jihadist-hacker-killed-us-air-strike-recruiter-pentagon-203051783.html (access: 04.06.2016).

5 | The Tallinn Manual, p. 119, footnote 63, which cites these three conditions stipulated by International Committee of the Red Cross.

2. Causal Link. There needs to be a direct causal relationship between the act and the harm involved in the first condition. Attacks that do not meet this criterion are labelled "indirect participation" and will not open the door to targeting the individual.
3. Belligerent Nexus. The cyber operation needs to be about the conflict, as opposed to a random cyberattack that takes place during a conflict but is unrelated (i.e. ransomware, PCI theft, espionage).

A Decision Tree for the Legal Targeting of Combatants and Civilians

The following decision tree has been constructed from the rules of the Law of Armed Conflict and International Humanitarian Law.

Is there an armed conflict underway that you are participating in?

If NO – STOP. You may not be targeted.

If YES, are you:
- a member of the armed forces
- a member of an organised armed group

If YES – you may be targeted.

If NO – have you carried out acts, which aim to support one party to the conflict by directly causing harm to another party, either directly inflicting death, injury or destruction, or by directly harming the enemy's military operations or capacity?
If YES – you may be targeted.

If NO – have you carried out acts directed against civilian objects (like a power plant) which had violent effects (such as a fire).
If YES – you may be targeted.

If NO – have you carried out acts that did not cause damage but did result in large-scale adverse consequences (like a blackout or a sustained Distributed Denial Of Service).
If YES – you may NOT be targeted as long as the collateral damage of your attack falls below the threshold described in Rule 30 of the Tallinn Manual[6] which states: "A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage to or destruction of objects."

The Case of Junaid Hussain

Junaid Hussain was a British hacker who joined ISIL in Syria and was actively involved in recruiting sympathisers in the West to carry out attacks. He also used his hacking skills in obtaining and releasing PII (Personally Identifiable Information) on U.S. military government employees. Hussain was targeted and killed by a drone strike on August 24, 2015[7].

The rationale was not a controversial one because Junaid Hussain's status was that of a DPH. His hacking activities may have raised his importance as a target, but it was not required to justify the strike.

The Anonymous War on ISIS

The online collective known as Anonymous announced that its members have declared war on ISIS after the attacks on Paris. By "war" they meant cyberattacks against ISIS/ISIL social media accounts and websites.

Assuming that the Islamic State had legal status as a nation state, and assuming that they could identify an individual hacker who participated in one of those cyberattacks, could they legally kill him?

6 | AFP, Jihadist Hacker Killed In U.S. Air Strike Was Recruiter: Pentagon, August 28, 2015 [online] http://news.yahoo.com/jihadist-hacker-killed-us-air-strike-recruiter-pentagon-203051783.html (access: 04.06.2016).

7 | AFP, Jihadist Hacker Killed In U.S. Air Strike Was Recruiter: Pentagon, August 28, 2015 [online] http://news.yahoo.com/jihadist-hacker-killed-us-air-strike-recruiter-pentagon-203051783.html (access: 04.06. 2016).

Let's work the decision tree and find out.

Step One: Is there a conflict underway? Yes.
Is the hacker a member of the Armed Forces? No.
Is the hacker a member of an organised armed group? No.
Therefore, under the Law of Armed Conflict, the Anonymous hacker cannot be legally targeted.

Let's proceed to his status under International Humanitarian Law (IHL).

- Did the cyberattack result in death, injury, destruction, or harm to the Islamic State's ability to carry out military operations? No.

- Was the cyberattack directed against critical infrastructure like a power grid which resulted in a fire, or did it cause a blackout which resulted in casualties? No.

Neither the LOAC nor IHL would support ISIL's targeting of an Anonymous hacker who was only responsible for attacks against social media and recruitment websites.

The Ukraine Power Grid Attack

Several hundred thousand people in three districts in Ukraine lost power for one to six hours on December 23, 2015 while the country continued to be in a state of armed conflict with Russia[8]. The Ukrainian government suspected Russian hackers to be responsible but stopped short of blaming the Russian government. It is likely that the attack was a work of hackers[9]. If one or more of those hackers were identified, could they be legally targeted?

Is there an Armed Conflict underway? Yes.
Is the hacker a member of the armed forces or an organised armed group? No one knows who was responsible for the Ukraine power grid attack but for the purpose of this example, let's say the answer is yes. Then, that hacker would be considered a DPH and could legally be targeted.

If the hacker was a civilian, did he carry out acts against critical infrastructure [YES];

- which had violent effects? [NO]
- which resulted in a blackout? [YES]

Based on current international law, the civilian hacker or hackers responsible for the Ukraine blackout may not be targeted because the effects of their work did not rise to the level required to justify lethal action.

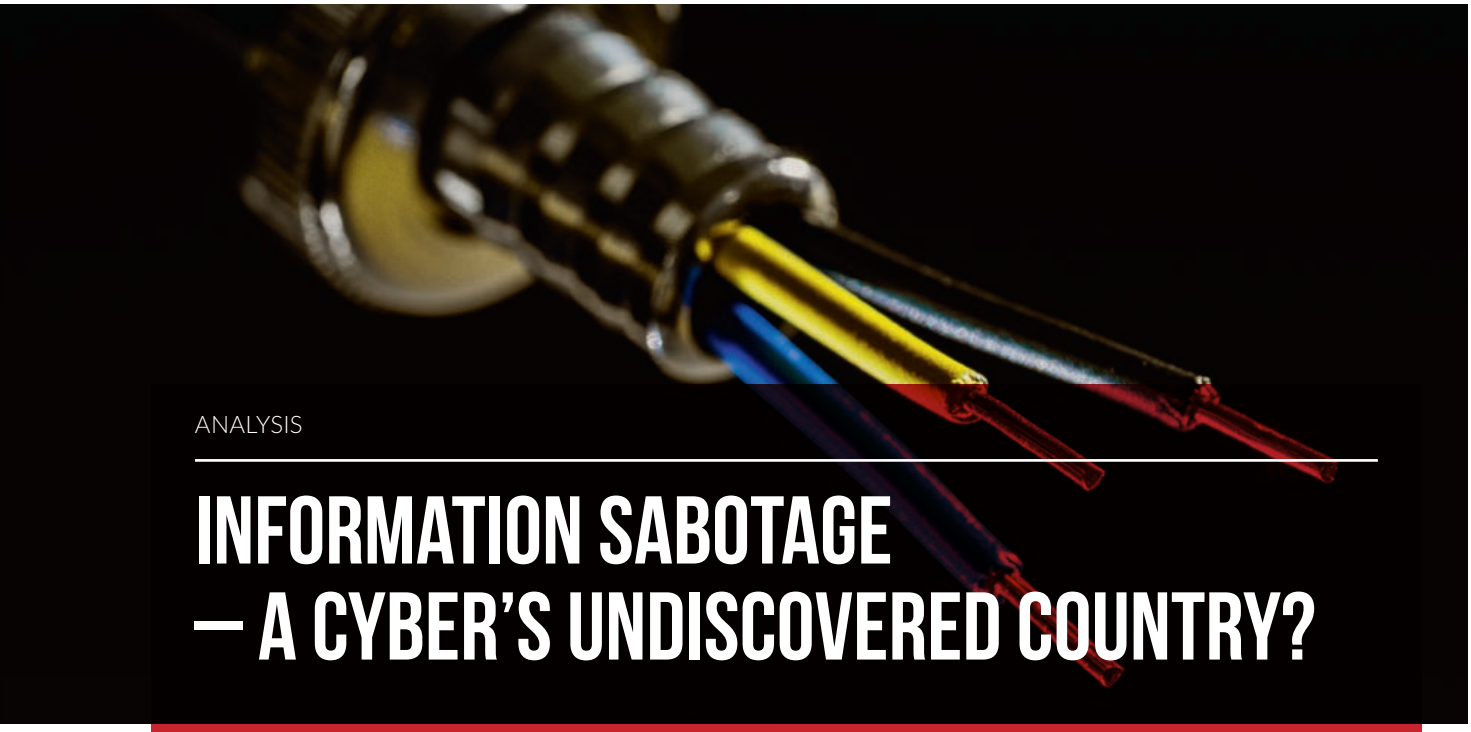
Conclusion

As the world's critical infrastructure becomes more interconnected by and reliant upon global digital networks, there is an increasing possibility that digital attacks upon those networks will result in effects that could cause harm to others.

> "As the world's critical infrastructure becomes more interconnected , there is an increasing possibility that digital attacks will result in effects that could cause harm to others.

If the level of harm is sufficiently high to meet the bar established under the Right of Self Defence in Article 51 of the U.N. Charter, or under International Humanitarian Law, then that civilian could be legally targeted. ■

8 | Politick P., Ukraine sees Russian hand in cyber attacks on power grid, Reuters, Feb 12, 2016 [online] http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VL18E (access: 04.06, 2016).
9 | This is the author's opinion based upon the minimal impact that the attack had on the energy substations networks. If the Russian military wanted to knock out Ukraine's power grid, they have the technical capability to cause massive and lasting damage.



ANALYSIS

INFORMATION SABOTAGE – A CYBER'S UNDISCOVERED COUNTRY?

JANI ANTIKAINEN
Jani Antikainen is a serial entrepreneur, venture capitalist, and a researcher at Jyväskylä University in Finland. His latest start-up, Sparta Consulting, focuses on protecting organisations' critical information assets from malicious manipulation. His academic research concentrates on identifying and countering data sabotage. Combining both academia and practical views, Antikainen develops comprehensive and powerful means for protecting both public and private sectors' information assets. He is finalising his dissertation in Economics and holds earlier M.Sc. in Economics and M.Sc. in Technology.

There has been an awakening. Something that was hardly ever mentioned – either by a name or described by different terms – is now under a special focus even in the eyes of the US chief intelligence officers. It serves well to examine this phenomenon, its mechanisms and effects to date, as well as those yet to be seen. Introducing: information sabotage.

What Are We Looking at?

In order to set the borders, firstly, it is good to take a look at what information sabotage is all about. Albeit, still used by security experts, the classic C-I-A triad, the confidentiality, integrity and availability (C-I-A) of information, already bears a notable patina and it might not give us the best possible framework to discuss information sabotage. However, the concept is so widely known that it still makes sense to examine information sabotage in the C-I-A context. Information sabotage sits most comfortably in the box of integrity, although it also touches confidentiality. It is likely that some information assets have been exposed to attacker, as well as availability – the main target of information sabotage can actually be adjusted to the timing of information flow.

It can be said that information sabotage compromises the integrity of information, but integrity itself is not a self-explanatory phenomenon. In short, high information integrity should be free of any tampering and thus reliable itself. This is all very good, yet we should really split the notion of integrity into two separate categories: form and fit integrity and functional integrity in order to better understand information sabotage and its guises. The integrity of form and fit refers to the way in which information (or data) "looks right" to an observer. The integrity of function

stands for the idea that information makes sense business-wise, that is, it respects the logic and rules of business.

Data without a context is just a data. Yet, as soon as data is put into a context, it becomes information; it is being perceived and used for making decisions or performing operations by a person (or machine) in specific situations. A specific situation of that kind gives us grounds to assess whether or not the information still retains its functional integrity. Without the context, there is only data.

> “However, the most difficult part is detecting attacks on business’ information integrity and ensuring that this integrity is not compromised.

Now, why is it worth elaborating on the integrity for a while, making all these rather fine distinctions? In this case, splitting hairs does give us a useful division line: one between technical integrity (form and fit) and business integrity (function) of information. However, the most difficult part is detecting attacks on business’ information integrity and ensuring that this integrity is not compromised. Activity that seeks to undermine technical integrity is something we can more easily detect and counter.

A prime example of how an information sabotage operation, resulting in compromised technical integrity of information, was carried out and eventually detected involves the Central Bank of Bangladesh and the Federal Reserve Bank of New York[1]. A group of criminals sabotaged the transactions’ data and orchestrated series of money transactions. Transactions worth 80 million USD went through, but at one point the criminals made a typo in a receiving party’s name (spelling “Shalika Foundation” as “Shalika Fandation”), which alarmed the routing banks to request for clarification of the name. This eventually led to the realisation that Shalika Foundation was a nonentity. An unlucky typo for the criminals, but a lucky one for the other involved parties. Information’s technical integrity compromise was detected, but instead of much functional integrity assertions, it was rather caused by a much sheer of luck.

As it was seen in the case of the Central Bank of Bangladesh, information sabotage aims at tampering with the information assets of the target in a way that affects, as the attacker desires, the target’s behaviour and the process of decision-making or operational activities. In short, it means a manipulation of the target’s information and, subsequently, a manipulation of its actions. An action like this can aim to cause inaction, i.e. the target’s operations might be delayed or even grounded to halt, meaning that it cannot operate or make decisions based on the sabotaged information. Indeed, it is what information sabotage is mostly all about. Bearing in mind the difference between technical integrity and business integrity of the information, we will refer to those notions later on.

Where Are We Standing?

Too many of cyber-related writings and opinions are gloomy and loaded with fear. Here I am going beyond existing schemes. Although facts, analyses and even wild future predictions are needed so that we can properly analyse risks involved in any threat or security phenomenon in general, we do not have to duplicate already existing attitudes, however, we are still left with plenty of uncertainty. What, then, do we have concerning information sabotage? First, information sabotage is not a new phenomenon per se. It has always been there. Yet, many thanks to the almost fanatical evangelising of several megatrends to the extent that they have

1 | Quadir, S., INSIGHT-How a hacker’s typo helped stop a billion dollar bank heist, Reuters 2016,[online] http://www.reuters.com/article/usa-fed-bangladesh-typo-idUSL4N16I4A8 (access: 16.05.2016).

almost become reality, giving information sabotage a very fertile ground to grow in. Digitalisation, the hyperconnected world, internet of things – the list extends further. With these developments and even more outrageous visions of the digital future, it makes sense to introduce the notion of information sabotage with that specific denotation; it reflects the times at hand and sets it into a context.

Second, until today the focus in the field of security of information and cybersecurity has been – referring back to the C-I-A triad mentioned earlier – C (confidentiality), I (integrity) and A (availability). This tendency is clearly visible in Mc Kinsey's article[2] on risks and cybersecurity, for instance, as it suggests that 'The theft of information assets and the intentional disruption of online processes are the most important technology risks that major institutions face.' At a later point in the article, same authors state that current models of protection against cyberattacks are becoming less effective and that they [...] are technology-centric and compliance-driven.' I could argue that those are not, perhaps, the most relevant risks but, nevertheless, the notion underlines the bias on the C (confidentiality) and A (availability) of information. It could be suggested that I (integrity) figures in this implicitly ('disruption of online processes' could be well carried out by information sabotage), but in more explicit terms. At least, it seems that integrity does not make the headlines here. I fully agree with the second notion that the concept of cybersecurity is a technology driven toll. There is a need for a change, if we are to counter information sabotage at its vilest – to compromise business' information integrity. Current IT mindset and technology can do very little, if anything, to tackle the challenge – they are only set to evaluate and ensure the technical integrity of information. The third point to make in this discussion – and this is good news – is that the tide is turning. Integrity, the reliability of information of both technical and business integrity, has drawn the attention of some rather important figures. The opinions on cyber's possible future from three of these people deserve to be quoted here.

US Director of National Intelligence, James Clapper[3] – 'I believe the next push on the envelope is going to be the manipulation or the deletion of data which would of course compromise its integrity;'

FBI Director, James Comey[4] –'Increasingly, we're worried not just about the loss of data but the potential manipulation of data, the corruption of data;'

NSA Director & US Cyber Command Commander, Michael Rogers[5] –'Our system – whether it's in the private sector or for us in the military – is fundamentally founded on the idea of trust of the data we're looking at.'

> "Information is the core asset of almost any institution; its integrity is of utmost importance. Manipulation of this core asset is something we are not prepared for.

These statements, coming from top intelligence officers of one of the most powerful nation states

2 | Chinn, D.,Kaplan, J., Weinberg, A., Risk and responsibility in a hyper connected world: Implications for enterprises, Mc Kinsey 2014, [online] http://www.mckinsey.com/business-functions/business-technology/our-insights/risk-and-responsibility-in-a-hyperconnected-world-implications-for-enterprises (access: 16.05.2016).

3 | Ackerman, S., Newest cyber threat will be data manipulation, US intelligence chief says, "The Guardian" 2015, [online] https://www.theguardian.com/technology/2015/sep/10/cyber-threat-data-manipulation-us-intelligence-chief (access: 13.05.2016).

4 | Comey, J.B, Speech on April 26, 2016 at International Conference on Cyber Engagement, Georgetown University, 2016, [online] https://www.fbi.gov/news/speeches/privacy-public-safety-and-security-how-we-can-confront-the-cyber-threat-together (access: 10.05.2016).

5 | Groll, E., Cyber Spying Is Out, Cyber Lying Is In, "Foreign Policy" 2015, [online] http://foreignpolicy.com/2015/11/20/u-s-fears-hackers-will-manipulate-data-not-just-steal-it/ (access: 10.05.2016).

in the world, provide a strong and unanimous message: information is the core asset of almost any institution; its integrity is of utmost importance. Manipulation of this core asset is something we are not prepared for and this threat will be most likely trending in the near future.

Within a single year, there has been a dramatic rise in awareness about the concept of information sabotage and its negative potential – "what-if-scenarios." If I were to have had a conversation with someone on the matter, say a year and a half ago, it would have been a monologue – even with people working at the very core of information security and cyber phenomena. During the summer of 2015, there was a notorious Office of Personnel Management (OPM) case, on which I ,along with Pasi Eronen, wrote an article on Overt Action[6], posing the following question: instead of stealing the circa 22 million security clearance person records, what if the criminals sabotaged parts of the personnel information over long period of time and created a situation in which we could have trusted none of the 22 million records, not being able to recognise which ones were trustworthy (business integrity), and which ones were sabotaged and thus misinformed. The national effect of such a scenario was speculated along with several other scenarios in which the worst thing was not the theft, but the sabotage of information. In many cases, nothing is worse than the loss of trust.

Within less than one month since publishing the Overt Action article, Clapper gave his testimony before the Congress, underlining the data sabotage risk. A few days after this, the Washington Post[7] connected these two dots: the possible OPM information sabotage scenario and Clapper's statement. Soon, several actors of the media, like the Foreign Policy[8], for instance, were taking an interest in the matter, and in a rather short time the rest of the US intelligence community followed suit with supporting views and statements like the ones quoted above. Of course, all of this should be taken as a progress for the good.

The Potential of Information Sabotage – the Past, the Present and the Future

Just like stealing information (C – confidentiality), denying access to it (A – availability), or information sabotage (I – integrity) will, hopefully, take a little bit of time before its full potential will be realised through several major attacks to get to the intended goals. It does not mean that there are no cases of information sabotage that become public on the verge of this digital era of ours. There are several cases and, unfortunately, on a rather big scale. Perhaps, the best known case of information sabotage was the good ol' Stuxnet, a textbook example, if such textbooks existed, of a successfully executed information sabotage. There is a hint of irony or cunning planning involved with the case since Stuxnet was, with high probability, created by the US (Israel's involvement in a joint operation has been a point of intense speculation) – the same country that now declares information sabotage as, perhaps, the most adverse cyberthreat to its military and private sector. It can be argued that Stuxnet has accelerated the development of information sabotage methods and the arsenal of weapons. It might also be asked whether the US should have opened that Pandora Box or should have left it unopened.

6 | Antikainen, J., Eronen, P., What's Worse Than Losing Your Data? Losing Your Trust In It, "Overt Action" 2015, [online] http://www.overtaction.org/2015/07/whats-worse-than-losing-your-data-losing-your-trust-in-it/ (access: 11.05.2016).

7 | Davidson, J., Manipulation of feds' personal data is a major danger in OPM cyber-heist, "The Washington Post" 2015, [online] https://www.washingtonpost.com/news/federal-eye/wp/2015/08/18/manipulation-of-personal-data-is-a-bigger-danger-than-info-theft-in-opm-cyber-heist/ (access: 10.05.2016).

8 | Antikainen, J., Eronen, P., What's Worse Than Losing Your Data? Losing Your Trust In It, "Overt Action" 2015, [online] http://www.overtaction.org/2015/07/whats-worse-than-losing-your-data-losing-your-trust-in-it/ (access: 11.05.2016).

There have been claims that the attack on German steel mill in 2014[9] in which the attackers tampered with the blast furnace temperature sensors' and gas flow control motors' data resulted in overheating of the furnace and, in a consequence, its later melt down. The attackers' remote disabling of the furnace's shut down was another information sabotage attack with physical world repercussions – similarly to the way in which Stuxnet physically broke the uranium enrichment centrifuges by sabotaging the control information in those devices.

> "The year 2015 demonstrated us how information sabotage can be used to steal $1 billion from financial institutions from all over the world[10].

The year 2015 demonstrated us how information sabotage can be used to steal $1 billion from financial institutions from all over the world . The Carbanak cybergang's main methods of achieving their goal was to inflate account balances with more money than they actually had and then, maze banking operators by transferring the extra money via fraud transactions to accounts of their own interest elsewhere in the world. Information sabotage at its finest!

The number of 'successful' cases is flooding into the public with intensifying rate. The threats come in many shapes – we have already seen nation states, criminal organisations, criminals running solo, as well as digital activists. Their motives are pretty much the same as with any cybercrime – they seek to shake the power structures, to change the competition's set ups, to destabilise adversary nations' operations, financial or political environments, to make money or just a statement to show their hostile capabilities.

Unfortunately, information sabotage is also a very alluring tool for one particularly evil agenda – terrorism. It is likely that, in the coming years, we will see a rise in digital terrorism. The simple reason for this is that there is a huge dark potential in information sabotage; information is a power and whoever controls the information, controls much more than we can imagine. The spreading of misinformation has been demonstrated by Russian Federation during the Crimean war. The rest assured: where power potential is available, there will be those who will seize it.

For terrorist organisations like ISIS, this potential offered by information sabotage cannot go unnoticed and unexploited. Its power over the global financial system has been demonstrated (e.g. above-mentioned examples of cases). For terrorists, money is the fuel that keeps them going on. In the case of ISIS, much of the counter activities have been driven towards the goal of stripping ISIS off the money and thus hindering its operations and its growth. It just might be that ISIS will be eager to try new ways of getting absolutely needed money, thus turning their interest from oil to binary world of ones and zeroes. What ISIS does by spreading terror physically (e.g. through the attacks in Paris and Brussels), it can be achieved with much less risk of failure involved in digital channels. We know that physical and critical infrastructure can be affected by information sabotage the same way like political sentiments and citizens' trust in the society. With the use of little imagination, there are too many possibilities available for the darker side of the humanity.

There Must be a Way...

Both presented cases of Stuxnet and the Carbanak cybergang's '$1 billion campaign' demonstrate

9 | Riley, M., Robertson, J., Cyberspace Becomes Second Front in Russia's Clash With NATO, "Bloomberg Technology" 2015, [online] http://www.bloomberg.com/news/articles/2015-10-14/cyberspace-becomes-second-front-in-russia-s-clash-with-nato (access: 12.05.2016).

10 | Virus News, The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, "Kaspersky Lab" 2015, [online] http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (access: 12.05.2016).

some of the information sabotage's general characteristics. Understanding these characteristics will help when building defences against the threat.

First, these attacks tend to be well targeted, even pinpointed at the very weakest link of a delivery or supply chain seldom suspected as a liability. One example of this could be stopping a just-in-time production line. It can be achieved by sabotaging the packaging material manufacturer's delivery information (which hardly considers itself as a target for cyberattack) and thus stopping the packaging material flow to the production line. With very little leeway in timing from production stage to delivery and no storage space, the line will stop as effectively as by pressing a red emergency-stop button.

From putting the attack into practice to its identification, the information sabotage attacks can span over a long period of time. According to FireEye[11], it takes a company, on average, around 200 days to spot that its systems have been breached by a cyberattack, including all possible types of attack. Information sabotage can span much longer, but even with that 200 days or far less, say 10 days, the question presented is a difficult one: 'When was everything ok? To which point in time should we return to find the non-infected data?' It is likely that the target cannot pinpoint the day and hour when the sabotage started and, thus, full recovery is impossible which is due to the next characteristic of information sabotage.

Information sabotage attacks are subtle and go easily unnoticed. They masquerade themselves as normal activities of the operators. For an observer, the attacks do seem like legitimate daily operations carried out by legitimate actors (users and systems). There is no footprint of any malware since none is necessarily needed. Firewalls detect nothing unusual, like connections to command and control servers, network traffic shows no strange patterns, security information and event management (SIEM) systems are unlikely to detect any strange systems' or users' behaviour and will not necessarily be the latest shiny things, user entity behaviour analytics (UEBA) systems.

All of this comes back to the difference between information's technical integrity and business integrity. For technical integrity, the information looks right for the eye, and particularly for transporting information from A to B and assuring that it has not been changed during its transit via available tools, for example, strong encryption nor as the latest promise – the blockchain. Information sabotage targeting the technical integrity of the information, by stupidly changing the information randomly, for instance, would be rather easy to detect.

The challenge thus is the business integrity and information sabotage which aims to go unnoticed and which respects the form and fit requirements of the information it sabotages. It seems that, by all appearances, the only possibility to catch this master of disguise at work is to catch him red-handed.

Of course, this journey does not start at the IT department or by browsing security tools from vendors' catalogues. In fact, there are not that many solutions yet available to tackle information sabotage. It is not a matter of tactics, but it requires strategic and operational level activities not usually available in the IT department's list of services. The solution formula for this problem goes as follows: The very first step is to identify the information that needs to be protected from being sabotaged. The first common pitfall is to name information systems or applications, and in the worst case – servers – that need to be protected. It seems that many people do fall into it, particularly those who should be the information security experts. There is a hint in the term information security which goes unnoticed – information! One needs to focus

11 | Ibidem, Gnoll, E.

on the information itself – and, yes, it is abstract and thus difficult to handle – and not to regress to the more readily understandable physical aspects of the task at hand, i.e. the technology.

> “ The strategic thinking needed here is to support building a business perspective which would overlook all of data and information available, and then deciding which part of it is the most critical one.

The strategic thinking needed here is to support building a business perspective which would overlook all of data and information available, and then deciding which part of it is the most critical one. To protect everything is to protect nothing (Frederick the Great) – a maxim that holds true, particularly in our era in which data, the raw material of information, doubles in size at even increasing rate. A tool that I have used successfully is to think in the following pattern: from services to processes and from processes to information. This is an especially effective way to identify the information, which a critical infrastructure operator needs to protect in order to fulfil its core obligations during exceptional times, like placing the society under martial law. This business critical information represents 0.5-2% of the whole of the information assets the operator has. Furthermore, no systems or applications are mentioned here – the information is what does matter.

There is an example for elaborating on thinking on the service-process-information: an emergency of a supply operator, a pharmaceutical company. From the scope of 100 products it manufactures, it has an obligation to supply X-amount of 5 of them under martial law. In order to put it in simplified terms: this is their only critical service. Pinpointing this sole service is the basis needed to further discover the critical processes providing that critical service. It is highly likely that this involves sourcing of production materials, logistics, the running of a few production lines, let alone, several supporting processes and capabilities like ensuring that only legitimate people are getting involved in the processes (it is also a subject to information sabotage, e.g. someone creating a fake internal person with access to production is a possible scenario worth considering). Once the strategic services and their operational services are identified, the final identification step is rather simple – to pick up from the ocean of information available bits that are needed for running the identified critical processes. The rest is irrelevant for the critical services’ purpose.

The second step of the solution formula needed after identifying the business critical information is to create controls over that information for the purpose of being able to say whether the information is trustworthy or not. Here, again, we need the business knowledge, not the technology enthusiasts of the IT department. These controls are the tool for telling if, once again, the business integrity is in place or not. These controls can be perceived as rules according to which the ‘business’ operates on. Although these controls are unique to a specific institution, either public or private, and the ways in which it operates, certain controls are rather common in nature.

> “ The second step of the solution formula needed is to create controls over that information for the purpose of being able to say whether the information is trustworthy or not.

Following the example case of the pharmaceutical company, the controls that would ensure that no outsider gains physical or digital access to premises or critical information might be as follows:

1) A new employee cannot be created to the physical premises access management system without being enlisted in the HR system first.
2) The core information of employees in the HR systems and that of physical premises access management system must match, with the HR being superior to the physical premises access management system (i.e. changes originate from HR-function using the HR-system).
3) Segregation of duties must be respected when creating a new employee – the HR assistant may create a person and fill their basic data, but cannot release the person's information further, for example, to the physical premises access management system. The information needs the HR manager's approval. At the same time, the HR manager cannot create a new employee alone, but they need an HR assistant's co-operation and validation of information (and the other way around).
4) A new employee cannot be created in any system if the creator is not registered physically in the building. It is a simple, yet powerful control.

And so on – there can be 10-20 of these controls that are rather simple, but when combined together, they make a strong barrier against an attacker who would require physical premises access to execute the goal they had in mind (e.g. physically sabotaging materials and products). For the attacker to succeed, they would need to understand, rather thoroughly, the business logic, processes and working practices of the target; the organisation. A single failure on any of the controls would disclose the attacker immediately.

We have now walked through an exemplary solution to build defensive capability against information sabotage compromising the business integrity of the information – the more 'dangerous' form of information sabotage. It is time to wrap up.

Camera, lights, ACTION!

During our journey into information sabotage, we have become familiar with a rather elusive concept that it is, discovered the fact that it has always been here, and that the megatrends shaping the world around us have recently given it a fertile ground in which to thrive and blossom. We named a few cases in which successful information sabotage has been carried out with the result of compromising the business integrity of information to a dramatic extent indeed.

Those cases demonstrated the very nature of information sabotage attacks, namely that they are usually targeted attacks, difficult to detect, subtle in their activities and masquerading themselves as regular operators carrying out daily chores. They can remain undetected for a very long period of time and if eventually spotted, the damage done is hard to identify. Moreover, after such a period of time, it is difficult to state which information has been altered by a legitimate business' action and which one has been sabotaged which, even if identified, is very difficult to recover from.

It was argued that the current stack of security solutions has a very limited capability of detecting, not to mention controlling, information sabotage attacks. This is something that is hopefully changing due to the attention that important figures and the massive cases have brought on information sabotage. Nevertheless, no technical solution can handle information sabotage, as long as the strategic and operational activities related to identifying the critical information will be protected and no further business controls on this information are carried out.

In order to reach the capability to counter information sabotage and build resilience over it, the borders of 'business' and 'IT' need to fade, and information sabotage needs to be perceived from the perspective of business risks management. Special attention should be paid on risks and

scenarios possibly affecting the information vital to most business critical parts of the institution's operations, like no process keeps running and no service delivered without their heart blood – the information.

There has been an awakening.. ■

ANALYSIS

DANGEROUS WEB SURFING – "I WILL BE VERY SURPRISED IF THIS COMES TO LIGHT"

SOC EXATEL

Security Operations Center of the Exatel is focused on: developing and implementing cybersecurity solutions within customers networks using i.e. Fidelis Cybersecurity products; deliver incident response, penetration testing and consulting services including forensics, code reverse engineering and threat intelligence; supporting products provided by Exatel in "as a service" model.

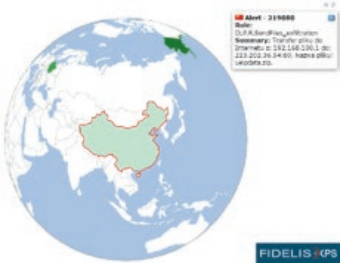
Exatel is leading telecommunication company in Poland, with 100% of Polish capital, focused on government institutions and enterprise customers. Exatel is a member of the PGE Capital Group – Poland's largest energy sector company with respect to sales revenues and net profit. Exatel manages Poland's state-of-the-art data transmission network with a throughput of up to 9,6 Tb/s in a DWDM backbone, boasting a network length of approx. 20,000 km. The company has a direct connection with nearly 80 of the largest national and 70 foreign operators, allowing for the transfer of data as well as the transit and termination of voice traffic routed through Central Europe.

The choice of a web browser is often a spontaneous activity. While searching for the content which is of our interest while using the Internet, we reach for popular surfing tools without thinking too much about them. As it turns out, this is not always secure... Such choices may entail severe and grave consequences for users and companies they work in. An example of this type of tools is the Maxthon 4 browser – according to the data from the year 2014 provided by StatsMonkey – the sixth most popular web browser used in Poland and China.

It is clearly indicated how risky can be the use of this browser by the result of a report on the technical analysis conducted by third-line analysts from the Exatel's Security Operations Centre. The report was drawn up based on an incident which was identified by the incident response team operating as a part of the Exatel's SOC at the end of March, while implementing the Fidelis threat detection system.

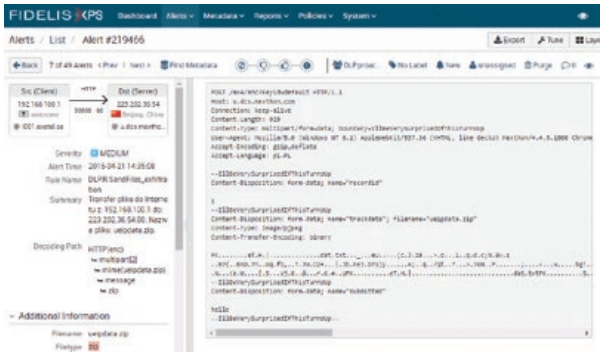
Owing to the information obtained during the analysis conducted using the code reverse engineering, the incident response team at the Exatel's SOC managed to reach the functionality which the authors of the Maxthon browser tried to embed in the software in order to send to their servers contents regarding the browsing history, Google searches and lists of software vulnerable to attacks, installed on the users' computers. What is important, the users of the browser were not aware of the fact of abuse, and even more, they were reassured by the manufacturer that the data will not be transferred anywhere without their explicit consent.

Soon after the internal LAN network of the organisation was connected to the Fidelis system for the purpose of monitoring, incident response team from the Exatel's SOC started to register from several to several dozens of alarms per day regarding the violation of the DLP.sendfiles.exfiltration rule, which was implemented by the Exatel's SOC into that system for the purpose of monitoring whether documents – in general, broadly understood data – are not sent outside the web by means of the HTTP protocol and the POST method. This is actually how web browsers transmit various data to remote servers including, for instance, files attached to messages sent using a webmail. It turned out that a small file bearing the name ueipdata.zip and weighing several hundred bytes is sent regularly via this protocol to a server in Beijing.



The Fidelis system implemented at Exatel is provided with the network memory module which not only collects the metadata, but also the details of any transmission which violates the security policy in any way. It is able to remember and carry out an in-depth analysis – using the DPI (Deep Packet Inspection) – of both the communication protocols and diverse encoding methods of the files nested in protocol payloads. Owing to this, the security experts from Exatel have full knowledge about any possible violation at their disposal.

The screenshot from the event monitoring console of the Fidelis system, which is shown above, presents the details regarding a single alarm generated as a consequence of violation of the previously mentioned rule, describing the potential exfiltration of data to the server in China.



The thing that attracted the attention of the specialists from the SOC was the fact that the sent ueipdata.zip file contains a single zipped dat.txt file, which is not a text file, but rather it comprises data with large entropy, being either an output from the random generator, or a result of encryption. Furthermore, the type of the file sent – identified by the content-type field of the HTTP protocol – was labelled as image/pjpeg, that is... an image:

However, the most surprising was the phrase which appeared several times in the content of the sent HTTP packet and contained the following text string: "IIlBeVerySurprisedIfThisTurnsUp".

Under these circumstances, the first and probably the most obvious subconscious translation of the phrase was: "I will be very surprised if this comes to light." Taking into consideration the fact that April Fools's Day happened to be approaching, the experts from Exatel's SOC initially thought that perhaps one of their colleagues was testing if the newly installed Fidelis system would be able to detect such an incident.

However, the translation of this phrase turned out to be wrong.

Further analysis of the coincidence of the name of the target server in China and the user-agent identifier recorded by Fidelis (the identifier which is usually used by the HTTP client for identification purposes) allowed Exatel's SOC team to reach the true offender and learn the proper translation of this phrase.

The offender that stood behind the alarms in the Fidelis system turned out to be the Maxthon web browser, created and developed by the Chinese.

According to the data obtained from the StatsMonkey service in the year 2014,

it occupies the sixth position with regards to popularity in both, Poland and China.

Rank	China	Market Share	%Market Share
1	Chrome	49.51	49.51
2	IE	28	28.00
3	Sogou Explorer	8.67	8.67
4	QQ Browser	4.56	4.56
5	Firefox	4.34	4.34
6	Maxthon	2.59	2.59

Rank	Poland	Market Share	%Market Share
1	Chrome	47.44	47.44
2	Firefox	35.83	35.83
3	Opera	7.8	7.80
4	IE	7.27	7.27
5	Safari	1.02	1.02
6	Maxthon	0.32	0.32

StatsMonkey, 2014

It was the Maxthon browser installed on computers of three company employees which sent the files that were noticed by the Fidelis system. What adds the irony to the whole matter is that the creators of the browser inform on their website that it was created with the thought of ensuring security and privacy to the users in the light of scandals related to violation of the privacy by the American National Security Agency (NSA):

http://www.maxthon.com/blog/rightstarups-cloud-browser-with-muscle-security-startup-maxthon-caters-to-html5-users/

As can be read in the opinions on Maxthon, the users are really fond of this browser because of the fact that its creators do not share the data with the American National Security Agency (NSA):

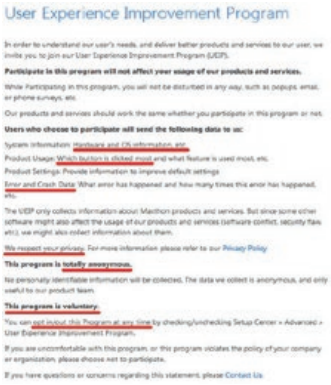
Coming back to the previously mentioned text string: "IIIBeVerySurprisedIfThisTurnsUp," which drew attention of the SOC analysts, its appearance in the transmission was the result of both a coincidence and a sense of humour of one of the Chinese programmers. He used such a static text string in the code of the C++ library (based on the MFC framework) to separate the files nested in the HTTP transmission – in our case, by instructing the Maxthon server how to decode the ZIP file in the HTTP packet.

The library which implemented the HTTP protocol client written by himself still in the year 2007:

```
261   void* pBuffer;
262   LPSTR szResponse;
263   CString strResponse;
264   BOOL bSuccess = TRUE;
265
266   CString strDebugMessage;
267
268   if (FALSE == fTrack.Open(_nFilePath, CFile::modeRead | CFile::shareDenyWrite))
269   {
270     AfxMessageBox(_T("Unable to open the file."));
271     return FALSE;
272   }
273
274   int iRecordID = 1;
275   strHTTPBoundary = _T("IIIBeVerySurprisedIfThisTurnsUp");
276   strPreFileData = MakePreFileData(strHTTPBoundary, pcmname, iRecordID);
277   strPostFileData = MakePostFileData(strHTTPBoundary);
278
279   AfxMessageBox(strPreFileData);
280   AfxMessageBox(strPostFileData);
281
282   dwTotalRequestLength = strPreFileData.GetLength() + strPostFileData.GetLength() + fTrack.
GetLength();
283
284   dwChunkLength = 64 * 1024;
285
286   pBuffer = malloc(dwChunkLength);
287
288   if (NULL == pBuffer)
```

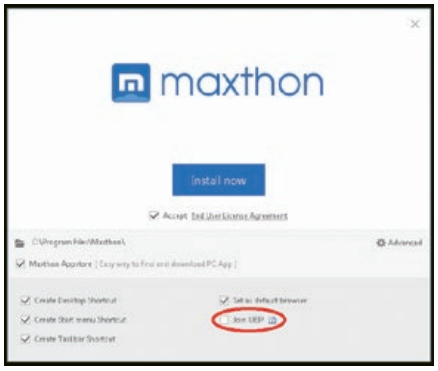
was used by the creators of Maxthon to create a part of the browser functionality. The true meaning of the aforementioned phrase was in fact: "I will be really surprised if this sequence of characters appears somewhere in the attached file sent by this program."

However we focused on the ueipdata.zip file, which repeatedly leaves the computers on which the browser was installed in strange circumstances and form. After a short investigation, the abbreviation – UEIP – was successfully deciphered as "User Experience Improvement Program." This is the name of the programme which, as the creators of the browser claim, is voluntary and anonymous, and its aim is to help the creators in improving the browser by sharing the information about: the hardware on which the browser is installed, the data concerning the operating system, and possible error and crash data reported during the functioning of the browser.



According to its creators, it is possible to resign from the UEIP programme at any time and "the privacy of the user is respected."

The Exatel's security experts decided to check this. They installed the Maxthon browser on their test machine, making sure that they had unchecked the option of participation in the UEIP programme on the startup screen:



Result? Unfortunately none.
The TCP traffic monitoring on the network interface of the machine during the use of the browser showed regular communication with the same Maxthon server: u.dcs.maxthon.com, containing the ueipdata.zip file in its payload.

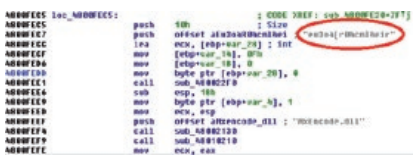
The specialists from the SOC were intrigued by several issues.

Firstly, why is the data of the UEIP programme transmitted to the Maxthon manufacturer despite the explicit lack of consent of the user?
Secondly, why is the ueipdata.zip file, which contains an apparently text file dat.txt that, in fact, is not a text file, sent further on pretending to be an image file?

Thirdly, what does the browser transfer to the Maxthon servers in the ZIP file?

The security experts from Exatel decided to investigate this matter in more details. For this purpose, they located the part of the code of the main process of the Maxthon browser that executes the data encryption command (the data that after encryption is saved in the dat.txt file, zipped into the ueipdata.zip file and transmitted to the Maxthon server). As they quickly noticed, the data is encrypted with a symmetric Rijndael (AES) algorithm, using a constant 16-Byte key – "eu3o4[r04cml4eir", statically compiled in the browser code, without using any kind of obfuscation.

The encryption key along with the plain text data buffer to be encrypted and its size, just before generating the new ueipdata.zip file and sending it to the Maxthon server, are provided as parameters in execution of Encode export function located in the Maxthon's dynamic library MxEncode.dll responsible for encryption of the UEIP data transmitted between the browser and the remote Maxthon server, and included in the ZIP files.



Analysis has shown also that the MxEncode library was created using the Crypto++ open source library which can be noticed in symbol table of the Maxthon's PE executable:

```
AVlogic _ error@std@@
AVlength _ error@std@@
AVout _ of _ range@std@@
AVtype _ info@@
AVbad _ exception@std@@
AV?$BlockCipherFinal@$0A@VEnc@Rijndael@CryptoPP
AV?$BlockCipherImpl@URijndael _ Info@CryptoPP@@VBlockCipher@2
AVexception@std@@
AV?$FixedBlockSize@$0BA@@CryptoPP@@
AVEnc@Rijndael@CryptoPP@@
AV _ Iostream _ error _ category@std@@
AV _ Generic _ error _ category@std@@
AURijndael _ Info@CryptoPP@@
AVNotImplemented@CryptoPP@@
AVAlgorithm@CryptoPP@@
AVDec@Rijndael@CryptoPP@@
AV?$TwoBases@VBlockCipher@CryptoPP@@URijndael _ Info@2@@CryptoPP@@
AV?$BlockCipherFinal@$00VDec@Rijndael@CryptoPP@@@CryptoPP@@
AVNameValuePairs@CryptoPP@@
AVNullNameValuePairs@CryptoPP@@
AVInvalidKeyLength@CryptoPP@@
AVInvalidArgument@CryptoPP@@
AVbad _ alloc@st
```

Further analysis demonstrated that the MxEncode library is also responsible for encryption and decryption of local Maxthon configuration files on the user's disk, which content is also protected by the manufacturer from the perspective of free viewing.

Taking the above-mentioned issues into consideration, the SOC experts from Exatel decided to monitor the communication between the Maxthon browser and its encryption module MxEncode.dll, and to conduct Man-In-The-Middle attack on the Maxthon encryption library.

They took advantage of the fact that in order to transmit the encrypted UEIP data to the server in China – Maxthon browser would first load the MxEncode.dll library located in its installation catalogue, transmit the data to be encrypted to the library (including the encryption code) triggering its export Encode function, and the library, after the data encryption, would return the encrypted output buffer to the Maxthon process, which would then transmit the already-encrypted data.

Thus, the experts from the SOC created their own DLL library which imitated the original MxEncode library, embedding their own two export functions – Encode and Decode – just like in the original form.

```
#include <stdio.h>
#include <windows.h>
extern "C" {
char mxEncodeDLLFile[] = "MxEncodeOrig.dll";
char encFile[] = "enc.dat";
char decFile[] = "dec.dat";
typedefint (*MxDecodePtr)(char *outBuf, char *inBuf,
```

```
 intbufSize, unsigned char *key);
typedefint (*MxEncodePtr)(char *outBuf, char *inBuf,
   intbufSize, unsigned char *key);
_ _declspec(dllexport) intMxEncode(char *outBuf,
   char *inBuf, intbufSize,
   unsigned char *key)
{
   HMODULE lib = LoadLibrary(mxEncodeDLLFile);
   void *ptr = GetProcAddress(lib, "MxEncode");
   MxEncodePtr MxEncode = (MxEncodePtr) ptr;
   FILE *f=fopen(encFile, "ab");
   fprintf(f, "[ENC.KEY] %s\r\n", key);
   fprintf(f, "[ENC.SIZ] %d\r\n", bufSize);
   fprintf(f, "[ENC.BUF] ");
   fwrite(inBuf, 1, bufSize, f);
   fprintf(f, "\r\n");
   fclose(f);
   return MxEncode(outBuf, inBuf,
     bufSize, key);
}
_ _declspec(dllexport) intMxDecode(char *outBuf,
   char *inBuf, intbufSize, unsigned char *key)
{
   HMODULE lib = LoadLibrary(mxEncodeDLLFile);
   void *ptr = GetProcAddress(lib, "MxDecode");
   MxDecodePtr MxDecode = (MxDecodePtr) ptr;
   int ret = MxDecode(outBuf, inBuf,
     bufSize, key);
   FILE *f=fopen(decFile, "ab");
   fprintf(f, "[DEC.KEY] %s\r\n", key);
   fprintf(f, "[DEC.SIZ] %d\r\n", bufSize);
   fprintf(f, "[DEC.BUF] ");
   fwrite(outBuf, 1, bufSize, f);
   fprintf(f, "\r\n");
   fclose(f);
   return ret;
}
BOOL APIENTRY DllMain(HINSTANCE hModule,
   DWORD ul _ reason _ for _ call,
   LPVOID lpReserved)
{
   return TRUE;
}
}
```

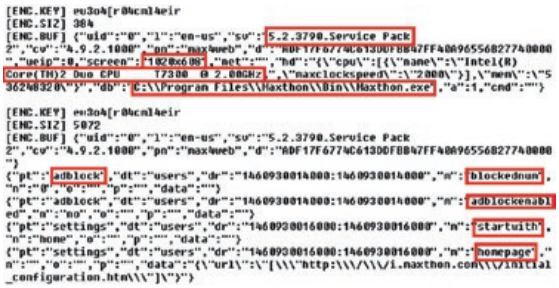
In both functions, they inserted the code that saved the data of every single Maxthon browser's encryption request on the disk, into a file indicated by them. After receiving the request for encryption and saving the data on the disk, the library provided by the Exatel experts should load the true Maxthon's encryption library (that was renamed to MxEncodeOrig.dll), triggering the relevant encryption function, and return the encrypted data to the Maxthon browser, which will thereafter transmit the data to the Maxthon server.

Thus, they allowed Maxthon to let all the data through their library which encryption would be required by the browser before its transmission to China. Using this method, aside of obtaining the entire already-decrypted UEIP transmission to the servers in Beijing, they also let Maxthon decrypt the configuration files, additionally capturing the decryption keys and the data

returned by the Decode function of the original MxEncode library.

Then, the browser was launched to check the effect.

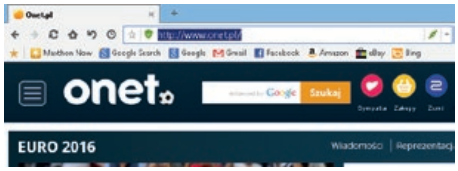
Just after Maxthon had been launched, it loaded the MxEncode library and requested encryption of the first data before its transmission, providing the experts from Exatel with the encryption key, which had been obtained during the prior analysis using the reverse engineering.

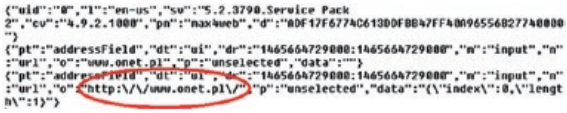


As can be seen, the transmission to the server contained: Windows Service Pack version, version of the Maxthon browser, screen resolution (of the virtual machine), type and frequency of the processor and local path in which Maxthon was installed on the disk. The values of configuration variables were also sent, namely: information whether the adblock was on or not, the number of already blocked ads and the website address of the home page.

The aforementioned data can be considered consistent with the list of information which transmission is mentioned by the authors in the description of the UEIP programme (leaving aside the fact that the user did not give their consent to join this programme).

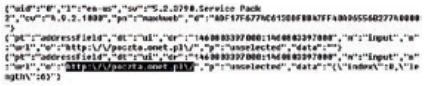
Then, as the Maxthon browser serves for the purpose of surfing the Internet – the experts from Exatel started browsing it. After visiting the first website,it was Onet for that matter, it turned out that the fact of visiting this website was also recorded and reported to the Maxthon server.



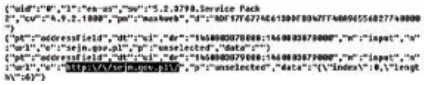


The same referred to information about each visited website.

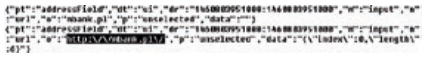
Logging to an e-mail account:



Visit on the website of the Polish parliament:



Visit on the Bank's website:



Thus, all queries by means of the GET method of the HTTP protocol were sent to the Maxthon server.

In short, what does it mean?

The entire user's website browsing history reaches the server of the Maxthon creators in Beijing, including contents of all the entered Google search queries.

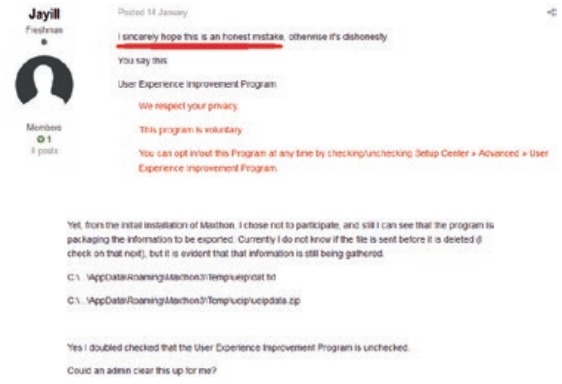
While continuing the web surfing using Maxthon with "encryption MITM mode" built in by the Exatel, the experts noticed that also the complete list of software installed on the computer, including precise version numbers, is transferred from their test machine

to China server, once in about five transmitted ueipdata.zip files.

In reality, this piece of information transmitted without the user's knowledge between the Browser and the Maxthon server allows to conduct a very precise targeted attack. By gaining knowledge about the user's website browsing preferences, information about his Google searches as well as the complete list of software installed on the user's computer, the attacker only needs an e-mail address to which he will send a message (authenticated by its content), containing an attached armed remote code execution exploit.

Additionally, due to another mistake committed by the creators, this time an error in the cryptographic architecture, the data which is transmitted without the prior authorisation of the user may be intercepted and decrypted by any potential attacker. All the attacker's needs to accomplish that is to "stand" between the user browser and the Maxthon server to intercept the communication. The intercepted UEIP transmission may be decrypted using AES symmetric keys, obtained from the Maxthon's binary code, after reverse engineering the code.

Thus, the experts from the SOC had good reasons to doubt the security of use of the Maxthon browser, just like its other users who noticed the ueipdata.zip files created on their disks.



The Maxthon user asking question on the official Maxthon browser forum received an evasive answer from the authors, that there are two different types of the UEIP programme.

The following request of the user, addressed both to the creators and to other users, for help in decrypting the attached exemplary ueipdata.zip file whose creation was noticed by the user on his disk.

The forum moderators deleted the link to the exemplary UEIP file, answering the user concerned about the contents of the encrypted UEIP files sent from his computer, that he will find the answers in the Maxthon privacy policy.

To sum up the above considerations: the Maxthon browser is not secure.

It allows conducting the targeted attack on a selected user by revealing the browser authors the complete list of exact versions of programms, some of which may be vulnerable, also providing them with user's browsing history and Google searches.

The use of the symmetric cryptography and static encryption keys embedded in the code to obfuscate the transmission of the UEIP data, actually allows to conduct the Man-In-The-Middle attack by any attacker, resulting in decryption of the UEIP data intercepted between the user's browser and the Maxthon server in Beijing.

It is also worth emphasising that the Exatel's SOC got in touch with the creators of the Maxthon browser, sending a detailed technical report, with a request for Maxthon to respond, either in the form of a notice sent to the users about the type of data transmitted from their browsers to the Maxthon servers in Beijing, or in the form of a Maxthon browser software patch which would enable the alarmed users to deactivate effectively the transmission of the UEIP files to their servers. This request was ignored.
The latest version of the browser downloaded from the creators' website (version 4.9.3.1000) was tested by the Exatel's Security Operations Centre team and still transmits the UEIP data, without respecting in any way the user's choice regarding the participation in the UEIP programme. Until the delivery of this text for publication, nothing has changed. ■

EUROPEAN CYBERSECURITY FORUM

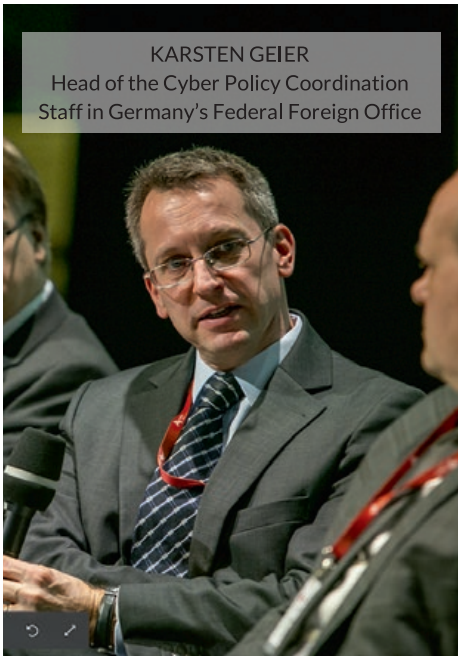
Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

26-27 September 2016, Kraków, Poland

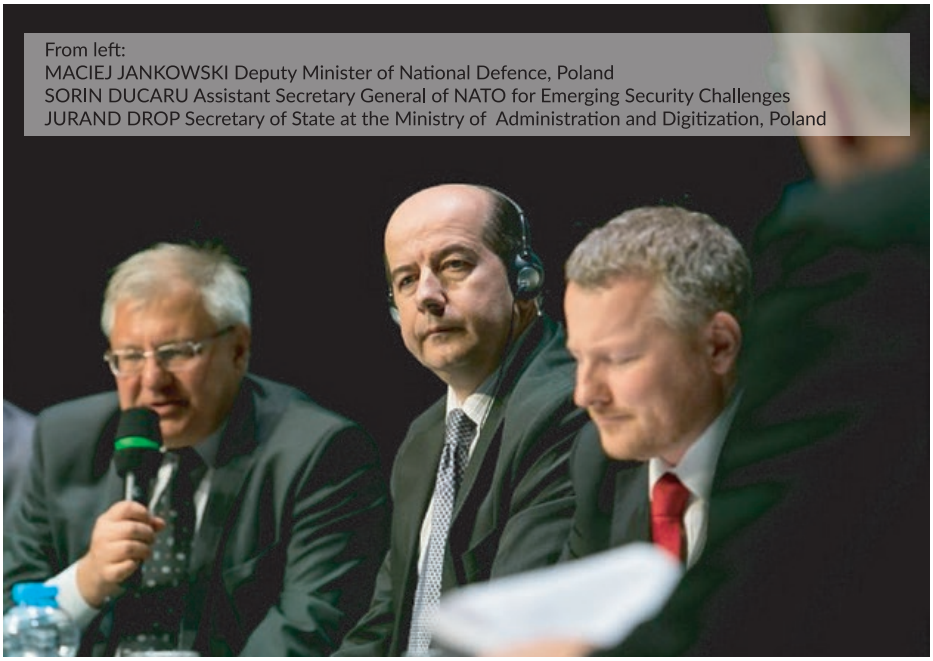
CYBERSEC 2016

STAY TUNED

WWW.CYBERSECFORUM.EU



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



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

AMBASSADOR SESSION

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

PAUL NICHOLAS
Senior Director at Microsoft HQ Redmond

CYBERSEC AUDIENCE

OPINION

OPEN AND SECURE – THE ROLE OF THE INTERNET STANDARDS IN GOVERNING CYBERSPACE

ROBERT SIUDAK
International Project Coordinator in the Kosciuszko Institute responsible for CYBERSEC HUB and CYBERSECtest.pl initiatives.
PhD candidate at the Jagiellonian University, previously a student at the Tel Aviv University and Trinity College Dublin.
His main scientific interests are: security studies, cyberspace and interdisciplinary approaches to security.

Introduction

The Internet standards are like grammar rules – indispensable and at the same time invisible as long as everything works smoothly. We use them every day to facilitate our basic on-line activities. We check our email, we use online bank account and we order groceries from the website of our favourite stores. The Internet standards are those funding blocks which make it possible and secure.

> “ The Internet standards are those funding blocks which make it possible and secure.

But we should not take it for granted. It is important to be aware that the way cyberspace, especially the Internet, works today is neither ultimately established nor even set in stone. Cyberspace is evolving as one of the most rapidly changing spheres of the international co-operation. We are witnessing a clash of competitive ideas about the future online reality. In the wake of this fundamental discussion, it is important to stress the key role of the up-to-date internet standards as a technical solution and most appropriate answer to the dilemma of “secure vs. open network.”

One internet, two visions

We already know that the year 2016 is going to be remembered as critical in the process of establishing model of international governance over internet. By the end of September 2016, The Internet Assigned Numbers Authority (IANA), an organisation responsible for allocation of IP numbers, management of Domain Name System (DNS) and internet protocols will terminate their contract with American government, namely the US National Telecommunications and Information Administration (NTIA). Since 1998, IANA and their public international representative – the Internet Corporation for Assigned Names and Numbers (ICANN) have been linked with NTIA through series of contracts. In the face of growing international pressure and controversy over Edward Snowden’s revelations, the US government decided to terminate institutional links with IANA.

The quest for a new model of the internet stewardship has emerged. Between March 2014 and 2016, more than 1100 meetings around the world and 590 webinars were debating on IANA transition. ICANN with the support of the US, the EU and many other countries and organisations suggested the model of multistakeholder governance. It is based on inclusive, diverse platform open for the participants from all sectors:

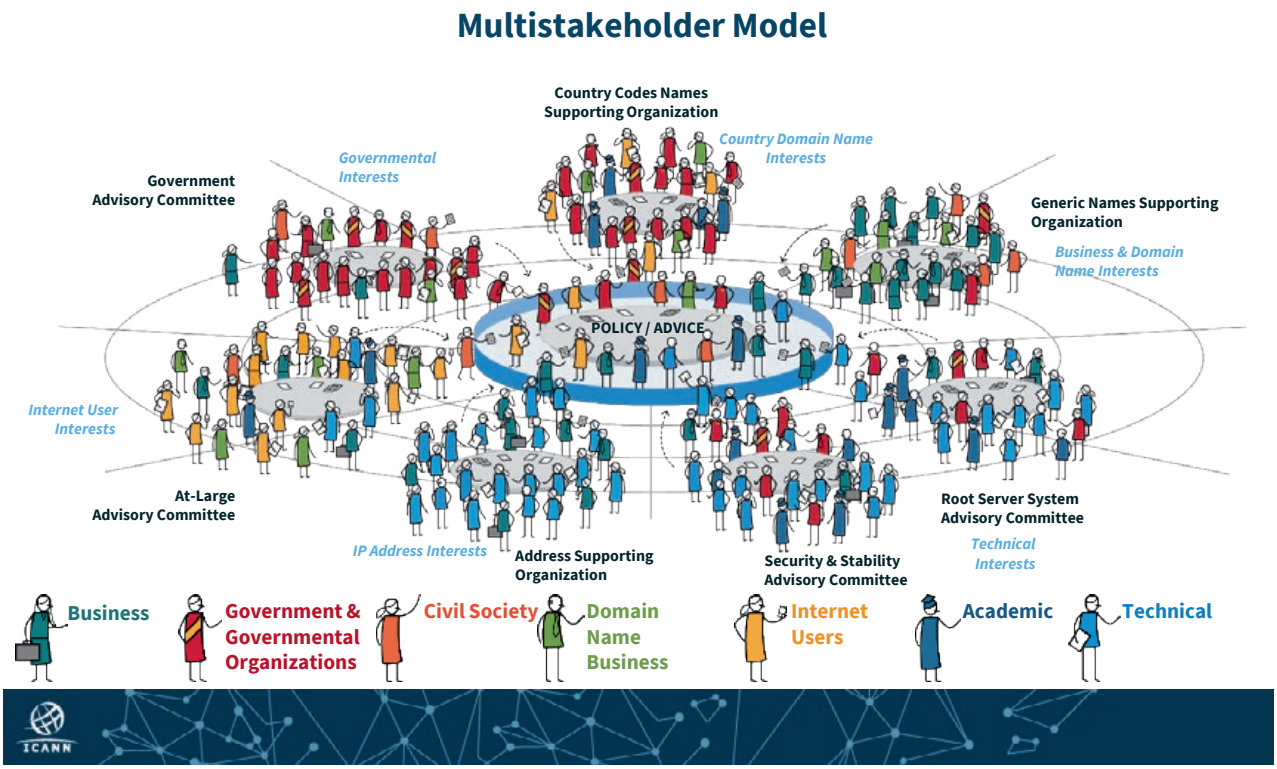
- Businesses;
- Civil Society;
- Internet Users;
- Technical;
- Academic;
- Domain Name Business;
- Government and Governmental Organisations.

On the 9th June 2016, NTIA published a long awaited report appreciating the efforts of

ICANN and opening the way for the transition of the stewardship to the multistakeholder platform coordinated by ICANN:

"Like the Internet itself, the multistakeholder model is characterized by its open participation and decentralized processes. The Internet thrives only through the cooperation of many different parties. The multistakeholder model reflects this fact by enabling a diversity of stakeholders to participate, fostering a diversity of opinions and ideas. (...) In recognition of this, the U.S. government is a staunch supporter of the multistakeholder model[1]".

There is also an alternative model on the table promoted by China, Russia and to some extent by countries such as Brazil or India. This intergovernmental approach developed by members of Shanghai Cooperation Organization calls for a key role of states, diminishing at the same time other stakeholders such as technical, business or academic organisations. This position is based on a view that only Chinese or Russian government is the sole legitimate representative of the interests and views of their societies or businesses. Therefore, intergovernmental proponents call for the transition of internet stewardship to the United Nations system and the establishment of a new UN body dedicated to the internet governance. Supporters of this stance emphasise



Picture 1: Multistakeholder model. Source: ICANN

1 | National Telecommunications and Information Administration, U.S. Department of Commerce, IANA Stewardship Transition Proposal Assessment Report, June 2016, p. 2 [online] www.ntia.doc.gov/files/ntia/publications/iana_stewardship_transition_assessment_report.pdf (access: 03.07.2016).

also unequal position of non-western stakeholders within ICANN model due to the lack of resources and historical development of the internet infrastructure within the US. The intergovernmental narration is strengthened by the idea of cyber sovereignty promoted especially by China. During the second edition of the World Internet Conference organised in December 2015 in Wuzhen, China, Xi Jiping, President of the People's Republic of China stated that: "We should respect the right of individual countries to independently choose their

> Creating state silos in the cyberspace is not an answer to the growing number of cybersecurity threats, nor is it the way toward a safer internet.

own path of cyber development and model of cyber regulation and participate in international cyberspace governance on an equal footing[2]". At the same time, we need to remember that both the Chinese rhetoric and the actions regarding cyberspace are driven mainly by security arguments openly criticising freedom of the web as a source of societal and cybersecurity threats. The prime example of it is the Chinese Golden Shield Project known as the Great Firewall of China which allows the Chinese government to restrict and survey the flow of information within the Chinese cyberspace.

Taking all arguments propounded by the supporters of the intergovernmental model into consideration, we need to finally ask what kind of cyberspace they want to create. At the end of the day, this approach tries to impose traditional categories embedded in the power politics of the state system onto cyberspace. This is threatening fundamental properties of the Internet such as open standards, voluntary collaboration, integrity and global reach[3]. Creating state silos in the cyberspace is not an answer to the growing number of cybersecurity threats, nor is it the way toward a safer internet. Raising cyberborders will not allow us to build a strong and reliable global web. In opposite, it will create many excluded areas, weak and vulnerable blank spots available for those who want to use cyberspace for malicious intentions. At the same time, it will endanger the basic principle of the Internet by discrediting the sole idea of a World Wide Web.

Collaborative Security

The complexity of cyber realm requires multidimensional, cross-border co-operation of all key stakeholders. Our global interdependency in the online world forces us to work together on the creation of a reliable and resilient web infrastructure.

We have to face the fact that no one can be ultimately secure and no one can live in the isolated cyberspace. This uniqueness of the internet phenomenon requires of us to think out of the narrow box of security as a realm of borders, guards and surveillance. We need to apply a collaborative security paradigm[4].

> The complexity of cyber realm requires multidimensional, cross-border co-operation of all key stakeholders.

2 | Ministry of Foreign Affairs of the People's Republic of China, Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference [online] www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml (access: 02.07.2016).

3 | Internet Society, Internet Invariants: What Really Matters [online] www.internetsociety.org/internet-invariants-what-really-matters (access: 01.07.2016).

4 | Internet Society, Collaborative Security: An approach to tackling Internet Security issues [online] www.internetsociety.org/collaborativesecurity (access: 01.07.2016).

First and foremost, the collaborative security calls for building confidence among the internet users because, ultimately, people are those who create the cyberspace. They need to be sure that they can use secure, reliable and open internet for their private and public activities.
Secondly, in the interconnected online realm, the security of the whole system depends on the weakest link. The collaborative security approach recognises this fact and suggests collective responsibility as a way to encounter vulnerabilities of such structure. In this case, the scope of the responsibility extends to the system as a whole, which is not the same as to have every actor responsible for his part only.

> “ Founding principles of collaborative security paradigm find practical embodiment in the promotion of the up-to-date internet standards.

Both aforementioned founding principles of collaborative security paradigm find practical embodiment in the promotion of the up-to-date internet standards. New, secure and open standards, including DNS connected technologies, protocols and anti-phishing, anti-spoofing email support are the first line of the cyberspace defence system. In the internet environment we are facing both inward and outward risks. We can be a victim of a cyberattack but at the same time we can became an unaware participant of the DDoS or botnet action against other users. A systemic solution to such a dual threat will not be found in the political decision of creating yet another border but rather in a common technological effort to spread the best practices and safest standards across the whole web.

A collaborative security paradigm is finally founded on the fundamental human rights, the internet invariants and evolutionary approach based on consensus. This open, voluntary stance may create a problem of a so called “Tragedy of the commons.” Once again, the idea of multistakeholder platform which enables common stewardship across the borders may be pointed out as a practical solution. In fact, the last key feature of the collaborative security approach is the preference for bottom-up self-organised interest organisations rather than top-down government-led initiatives. In short: think globally, act locally.

Think globally, act locally: The example of Internet Infrastructure Initiative

Building a robust, open and resilient internet Infrastructure based on the up-to-date internet standards – that is the main goal of the initiative run by the Dutch and Polish stakeholders within the Global Forum on Cyber Expertise. This example of a bottom-up program raising awareness among web users falls within the collective security approach, strengthening openness and safety of the Internet.

The initial idea developed by the Dutch Internet Standard Platform took the form of internet.nl website where users can check whether their Internet is up to date. The project is promoting six modern standards for scalable and secure Internet use:

- IPv6 – an extended, modern range of internet addresses;
- DNSSEC – security extensions for domain names;
- TLS – secured connections;
- DKIM, SPF and DMARC – anti-phishing and anti-spoofing email extensions.

Internet.nl is already available not only in Dutch but also in English, and in the near future a Polish language version of the website will be in place. By establishing co-operation with the Kosciuszko Institute and the Netherlands Institute of International Relations ‘Clingendael,’ The Internet Standard Platform is now promoting exchange of

good practices and technological know-how. At the same time, the scope of end-users is widening, including people from countries such as Poland and the UK. As a next step of the initiative, the Kosciuszko Institute with the support of the Dutch partners will inaugurate a Polish domain operating under the name of CYBERSECtest.pl.

> Building a robust, open and resilient internet Infrastructure based on the up-to-date internet standards – that is the main goal of the initiative run by the Dutch and Polish stakeholders within the Global Forum on Cyber Expertise.

Within the Internet Infrastructure Initiative, other multiple simultaneous actions are also taking place such as seminars on the role of the internet standards in the digitalisation of public services in the EU[5] or campaigns for the obligatory introduction of DNSSEC on the governmental domains. All this within the model of multistakeholder co-operation including NGO's, technical organisations, business and governmental representatives.

Summary

Open and secure – there can be no compromises on any of these two characteristics of the cyberspace. Not if we want the Internet to retain its crucial role as a driver for economic growth, socio-technical evolution and cultural participatory revolution. That is why, instead of building cyber walls around our national cyberspaces, we need to co-operate on a long term infrastructural investments dedicated to the common interest of the internet ecosystem. Let there be no doubts – widely applied up-to-date internet standards will raise the level of web security much higher than any, even the most sophisticated cyber wall. ■

5 | Logius, iEU seminar: Digitizing European GovServices [online] www.logius.nl/languages/english/ieu-seminar-digitizing-european-govservices-june-6th (access: 02.07.2016).

INTERVIEW WITH DEAN VALORE

DEAN VALORE

Dean Valore (Juris Doctorate, Cleveland Marshal College of Law '99) is the Managing Partner of the Cleveland, Ohio law firm of Valore & Gordillo, LLP. Mr. Valore is also an Adjunct Professor of law at the Cleveland Marshal College of Law at Cleveland State University, USA. Mr. Valore previously served as an Assistant United States Attorney for the United States Department of Justice where he was a member of the Strike Force unit, prosecuting international organised crime and cybercrime investigations. He also led the Criminal Civil Rights unit prosecuting federal hate crimes and police excessive use of force cases. Mr. Valore has presented on federal anti-human trafficking laws and criminal civil rights and has lectured at the FBI Academy in Quantico, Virginia, on federal prosecutions of racially motivated hate crimes. He has participated in the U.S. Attorney General's advisory committee on international organised crime and cybercrime, and was honoured by the FBI and the Department of Homeland Security with awards of excellence in prosecution.

During your carrier as an U.S. Attorney, you were the Head of a team of Justice Department prosecutors, U.S. government and foreign agents. The result of your work was a successful prosecution of international cybercrime groups involved in internet auction fraud and money laundering schemes. How the Department of Justice adapted its work to this new challenge of cybercrime and what were the biggest obstacles?

The US Department of Justice has reprioritised its focus on investigating and combating international cybercrime since the events of 9/11. Many international cyberattack illegal proceeds are used to help fund terrorism across the globe and in America. Over the past several years, the Department increased its presence of federal agents assigned to investigate these crimes. Millions of dollars of government funding have been devoted to training agents and prosecutors in technological advancements, but one of the biggest obstacles is to keep up with the advanced hacking and scheming of the cyber criminals. It often seems that they are always one step ahead of the investigation, so that the work is always trying to catch up with the criminals.

Digital Age and connected to it threats forced the legislature to revised its traditional approach to crime. How this process looked in the U.S. and what kind of instruments, regulations are still missing?

Writing new legislation is always a slow moving process in our democracy. Many of the extraditional agreements with other countries are old and outdated and make it very difficult to effectively prosecute international cybercrime in the US. New extradition agreements removing or updating old world processes to bring these criminals to justice would make the work much easier.

Tor – initially developed as a tool for promoting democracy and freedom of speech in the internet, became a source of a great cyberthreat. How the American law enforcement agencies approach this problem?

Because America values the right to free speech so strongly coupled with the fast moving advent of social media provide a great source of work for federal law enforcement in combating cyberthreats. The American law enforcement had used the Patriot Act and enhanced listening techniques to monitor many forms of communication through the US. However, many in Congress have been opposed to this and change is afoot! Outside of the scope of terrorism investigations, free speech on the Internet will continue to be respected by the US law enforcement.

As a federal prosecutor, you were also a member of the National Security Unit where you were leading investigations and prosecutions related to domestic and international terrorism matters, involving terrorist financing and money laundering. You investigated and successfully

prosecuted immigration fraud cases. Based on that experience what in your opinion is the biggest difficulty in combating cyberjihadism?

The biggest challenges are infiltrating the cells and getting access to the inner workings. With the terrorists' use of social media, it makes it very hard for law enforcement to track and follow the trail.

Thank you for this interesting interview. ■

Questions by:
Magdalena Szwiec
The Kosciuszko Institute

OPINION

THE TRAP OF INFORMATION SECURITY" & ESCALATING CYBER RISK

JACK WHITSITT
Jack Whitsitt is a senior strategist at EnergySec. During his 14 years activity in both Information and Cybersecurity worlds he has written open source honeypot tools and operationalised security data visualisation theories. He had national control system incident response responsibilities, led large scale public/private risk management initiatives on behalf of the government, occasionally giving advice on international policy matters. He also teaches his own class at EnergySec on using frameworks to bridge the business/technology risk divide.

In the modern world we have come to accept that cybersecurity concerns are a fact of life. Whether we are wearing the filters of a seasoned general, a government leader, a software engineer or just a regular person, we know that cybersecurity matters to us. This has resulted in the development of a massive "Information Security" industry, new laws and policies, changes in insurance industries, and even Hollywood film and TV series. But has this progress been helpful? Of course any progress that moves the state of the world forward must have some positive elements. But will it get us to where we want to be? Likely not.

This is because, presently, "Information Security" is helping to perpetuate and escalate cyberconflict, not reduce it.

How can this be? Information Security, after all, gives us more weapons with which to defend ourselves and almost every conversation in almost every cybersecurity forum revolves around creating better defenders and tools: Bastion defence positions, arms, intelligence, logistics of responses, attribution, etc. are all at the forefront of cybersecurity thinking.

There appears to be in this thinking, though, an assumption of long-term sustained conflict. Little thought, if any, seems to be given to sustained reduction of exposed surface area, enabling rapid risk pivoting in socio-political institutions or partnerships, or what a (cyber) secure world would even look like.

What would it look like? It's actually hard to discuss in terms of "Information Security" because, as a pseudo-discipline, it presents strategists with several framing problems that must be examined to understand the nature of cybersecurity risk and how it can be reduced – and the appropriate model to use is not necessarily obvious. We've been getting it wrong for a long time.

For instance, the idea of networks or perimeters being "broken into" by "hackers" is no longer a helpful framework for understanding cybersecurity. Instead, strategists should consider cyber risk to be a parasitic problem space. In this space, entities compete for the use of common systems to produce value – some of them legally, others not.

> "There are no individual networks or infrastructures any longer.

It is helpful here to understand that there are no individual networks or infrastructures any longer. If an entity "purchases" or "builds" a "system," what they are really doing is adding components to a single internet; they are not building their own "networks." These entities might then have the "legal" authority to use their section of the internet to produce value, but it is not a separate system.

When subsequently examining what "risk" and

"hacking" and "cybersecurity" look like on this modern, shared internet, it should be clear that our "adversaries" resemble parasites attempting to hijack our collective infrastructure in order to attain their own ends. These ends might include halting the legitimate value being produced, altering it or generating entirely new outputs. In all cases, however, there is a sustained competition between all parties for value production. Further, the only difference between legitimate entities and "adversaries" is a matter of legal perspective and faith in ownership of systems that are not really separate from each other.

> "The idea of individual incidents being the focus of security efforts is less than helpful.

This situation has several implications for managing security.

1. The idea of individual incidents being the focus of security efforts is less than helpful. The internet exists in a constant state of compromise, conflict and risk. There may be individual "infestations" of a subsection of the internet, but those are often tangential to the overall health of the underlying system. An excessive focus on managing these infestations can hinder a more useful focus on the management of factors affecting the entire system.

2. Security cannot be achieved by independent entities alone. It is simply not possible. There are massively matrixed supply and trust interdependencies involved in every aspect of the internet. When managing a parasitic problem, the collective components of a system must work together to reduce the exposure area so that the likelihood and associated costs of actual infestations are manageable over time. Without collaboration and co-operation across "legal sub-component" boundaries of our infrastructure which are the most fundamental requirements, the surface area needing management by individual entities will continue to increase with every line of code written, every additional connection made and every new user – but without the benefit of economies of scale and shared resources applied to the collective problem sources.

3. "Adversaries" hold several high points as opposed to "legitimate" system owners. Adversaries are not always bound by the same "soft" constraints as others (i.e. law); they are able to utilise and exploit single exposure opportunities over time without being required to hold a constant line (thereby allowing more flexible resource utilisation), and have (whether in league with each other or not) collective impact on the resources and environmental stability of "sub-internet system owners" who are often prevented from collaborating by political, legal, and cultural barriers.

4. When cybersecurity is looked at as a value-production competition in a parasitic environment, it should be very clear that the goal of cybersecurity is not "security." In fact, there is no such thing as "cybersecurity" as a strategic goal. Instead, "cyber" goals are intrinsically and unavoidably tied to our existing value production goals. This means that any efforts to improve security sustainably that do not include value production mechanisms in their scope are doomed to fail.

> "Any efforts to improve security sustainably that do not include value production mechanisms in their scope are doomed to fail.

5. Most importantly, cybersecurity is a human-driven state that encompasses both human and

technical systems. There are no security states that are not created by an aggregate series of authorised decisions by people in authorised roles somewhere on a timeline. Humans are the sole causal factor in our cybersecurity risk and any attempt to reduce risk that does not acknowledge improving decision-making capacity as a primary goal is doomed to fail.

Taken together, these factors and perspectives demonstrate that our model of information security is severely broken. Entities are not – as most information security practices assume – individual defenders who can, with sufficient resources, willpower and effort, hold bad actors at bay indefinitely in a way that maintains their desired level of "security."

Instead, we are all under siege in a hostile environment by opposition that holds high ground and is difficult to dislodge. This is an important point. Few, if any, individual entities on the internet have or will ever have the visibility or ability to make effective risk based decisions. The scope of their influence, ownership and resources – whether industry, government, or citizen – is simply not broad enough to manage all of the variables involved in breaking a siege. Left in isolation, entities are forced to do the best they can in the fact of the escalating costs associated with increasing complexity against a broad mix of adversaries who face massively different constraints which are, broadly and asymmetrically, in the adversaries' favour.

Unfortunately for everyone, "information security common practices" are not effective at coping with any of this. These are common practices as we know them today:

1. Treat companies as defenders and so create a continuous mismatch between expectation and capability. Attempting to enable a company's ability to fight off a single attack might make sense. But that's not what is happening. Instead, those attacks (and, importantly, the simple possibility of those attacks) are putting funded, thoughtful, sustained, direct and indirect pressure on organisations. This requires different kind of resource commitments and capability competencies. Few, if any, organisations are able to sustain them.

2. Require trust boundaries that assume a securable perimeter of control (if not a network perimeter) that poorly reflects the reality of operating in modern society. Attempting to apply secure authentication, authorisation, encryption, monitoring, code verification, etc. across every actual relevant trust boundary rapidly looks hopelessly tangled. This has the effect of isolating control authorities who should be collaborating into false perimeters and creating a resource black hole which can never be sufficiently filled with information security controls.

3. Focuses on managing individual (real or potential) incidents as opposed to removing the sources of systemic exposure introduction and instability. This obscures visibility into environmental risk and does not assure generally defensible organisational behaviour. Organisations can implement the world's most effective incident management controls and yet still introduce enough exposure outside the scope of "Information Security" controls to overwhelm their own capabilities.

4. Create situational awareness disconnects between stakeholder needs, actual exposure, and provided data. The NERC CIP regulations in the U.S, for example, are designed with no threat model in mind and, while they may or may not have an impact on the ability of adversaries to intrude into "networks" (as measured at single points in time), the regulations do nothing to provide government officials with knowledge of their

infrastructure's exposure to cyber risk or its overall defensibility against thoughtful, adaptable threats – and it is this knowledge that the US government most needs from its regulatory reporting in order to make effective diplomatic, policy and military decisions. As it stands, classic "Information Security" regulations serve neither the benefit of the regulated or the regulators.

5. Lack of direct connection to risk introduction sources. Almost exclusively scoped as a technology or technology support ("User Awareness Training") suite of practices and controls, "Information Security" rarely, if ever, provides levers for or insights into how entity decision makers (such as CEO's, Procurement Officials, Agency Leadership, etc.) are creating or should be influencing the state system. Instead, they attempt to compensate or unmanage system exposure introduction and are thus subject to (likely) more externalities than they can, by definition, control.

Taken together, these and the other limitations – at a minimum – hinder progressing sustained risk reduction. By investing (and entrenching) practices such as these, entities are expending valuable financial, political and cultural capital into efforts that lock them into constraints that work against their own interests and (by themselves) limit their ability to respond to thoughtful, funded, adapting adversaries and environments. Unfortunately, this is not the extent of the problem.

Attend any conference, framework development effort or international policy workshop and elements of information security practices will have snuck in under the guise of "strategy." For example, Industry, Government and Military leaders can often be found discussing the need for better "Information Sharing" and the impacts of "Vulnerability Markets" in cybersecurity. The massive misalignment of these topics with the roles and responsibilities of those developing long term strategies cannot be overstated. It is not only inappropriate but potentially fatal to a long term success.

Why? At best, "Information Security" practices are helpful at making us better at engaging in conflict. They neither provide the levers nor address the scope of problem space required to reduce cybersecurity risk over time.

> "Information Security" practices neither provide the levers nor address the scope of problem space required to reduce cybersecurity risk over time.

Not only that, but working strategy at this level does something impressively frightening to how we think of the problem: replacing "Information Security" tactics for real strategy removed the conceptual idea that the relationship between risk owners and their adversaries is something that can be strategically changed.

By focusing all of our resources on improving the types of tactics "Information Security Practitioners" engage in, leaders inadvertently are using their authority of power to limit cybersecurity strategy in a way that perpetually escalates conflict: as complexity increases beyond what resources can combat in terms of incident management, there will be sustained resource drainage while potential consequences to accumulate over time. This provides additional opportunities for adversaries to take advantage of a connected world, does nothing to de-incentivise the use of connected system hijacking as a strategy, and does not even provide risk visibility into our nations or industries.

"Information Security" undoubtedly provides necessary suite of tools and capabilities, but it is, as a discipline, not a path to success. There must be a vision, a plan and resources allocated toward breaking the siege we are all living under online.

It is easy to see how we arrived here and examining that process helps to explain why there remains such a fixation on such low-level practices and what barriers exist to realigning our strategic discussions to more appropriate elements of the problem space. Take, for example, any of the United States' proposed "Information Sharing" bills over the past few years. Why is their congress discussing such minutia? "Information Sharing" should be the type of capability that evolves out of strategy and into law; not forced. But, here is (partially) how that conversation evolved:

Years ago, the internet was largely an island unto itself. It had the occasional security events, but they were limited in scope of effect and concern. Technologists concerned with running the internet took note, but they largely had limited scopes of influence and no real dedicated security resources. To fill the gap, they began to develop practices that they could implement within their spans of influence.

Sometime later, additional – much more publicly interesting – functionality was added to the internet. People began to care what happened in this new space. Not long after, businesses began to experience a plague of automated worms and the real value was put at risk. A market need was identified and the technologist-developed practices began to be sold as solutions. This worked for a while because the worms attacking infrastructure were thoughtless; they more closely resembled natural weather incidents than adversaries whom static defences could and would pivot around.

As the information security industry expanded to meet this need, even more of our lives became connected to the internet – along with all of our associated conflicts and crimes. Automated worms began to give way to thoughtful adversaries, but there were two key problems:

1. The automated worm solution set had become an entrenched industry.
2. Thoughtful adversaries took advantage of how we did business – they exploited flaws in our decision-making capacities throughout government and industry – not just technical flaws.

Instead of being able to adjust our perspectives and expand scope, we fell back on what we had available and were unwilling to expand the scope of security in a way that influenced how we produce value. We allowed our adversaries' scopes to exceed what we considered attack surface and we have not yet shifted out of that mindset. Worse, in fact, we have dug in our positions and have attempted to wring the very last bit of capability out of a technology centric approach.

The failure of this approach can be easily seen in the obsession with information sharing. If businesses and governments are leaving the doors and windows open on a regular basis, the only solution is for our "defenders" to learn as much about the adversaries as possible and respond using threat-centric approaches. This leads to several (hopefully) obvious problems:

1. Someone has to be compromised before we know how we might be compromised in order to have information to share. That "someone" might be us – and on a shared infrastructure internet, that distinction might even be meaningless.
2. We really can't ever know all the threats out there and, more importantly, attempting to prioritise threat information as a key component of our strategies actually ties control of our long term decision making into the short term decisions made by adversaries. This is unsustainable, if it works at all.

Yet, despite these limitations, there is a number of "Information Sharing" bills proposed in the U.S. congress and huge volumes of materials dedicated to improving it. The tactics of practitioners have

risen up into the strategic tiers of "international decision makers."

Perhaps passing a few of these tactical laws will be helpful in shifting the discussion into deeper territory. As we enable better conflict, there could be room created for a new vision into the problem space.

> "With luck, new leadership over time will look at where we are, see the failings of "Information Security" as a strategy and develop a vision for reducing cyberconflict through innovative application of statecraft to the real barriers we are facing.

With luck, new leadership over time will look at where we are, see the failings of "Information Security" as a strategy and develop a vision for reducing cyberconflict through innovative application of statecraft to the real barriers we are facing. These barriers exist, in their most critical form, as cultural, legal and political limitations to how we make decisions, work together and build sustainable, resilient human processes and systems as whole societies – as opposed to individual enclaves of the "networks."

Until this happens, and as long as we continue down the path we are on, complexity will increase, investment will become more entrenched and the risk and conflict associated with connected systems will increase. ■

EUROPEAN CYBERSECURITY FORUM

The 1st Annual Public Policy Conference dedicated to strategic aspects of cybersecurity

28-29 SEPTEMBER 2015 - KRAKÓW, POLAND

CYBERSEC 2015

RECOMMENDATIONS

ANALYSIS

TRENDS IN JOINT NATO-EU CYBERDEFENCE CAPABILITIES

PIOTR K. TRĄBIŃSKI
Piotr Trąbiński is a cybersecurity expert at the National Centre for Strategic Studies. Mr Trąbiński is a former director of Santander Universidades Department at Bank Zachodni WBK. His area of research focuses on institutional and strategic implementation of cybersecurity capabilities, as well as technology and organisational transition in business environment. He is a graduate in law faculty at the University of Warsaw, and a former President of Bank Zachodni WBK Foundation.

Although NATO and the European Union are two different organisations dedicated to fulfil their missions, they still have certain fields of co-operation, especially on the level of common defence against rising threats. One of the growing concerns which equally threatens international organisations, countries, businesses, armies and citizens is cyberthreat. With increasing usage of data, internet of things, SCADA systems and IT running components which provide faster and more accurate services comes hidden danger of abuses in cyberspace. As long as both military and civil critical infrastructure elements run on digital software – even if it is not connected to the internet – each country and each organisation is obliged to assess their security. If an organisation wants to use IT driven systems with access to cyberspace and hold high level of network protection, then it has to co-operate with all other actors which share similar cyberthreats. It applies to businesses, government institutions and international organisations like NATO and the EU. Both NATO and the EU have already addressed some of the questions to mitigate the risks that come from cyberspace; at least some of them were addressed mutually and the co-operation between both institutions began. The purpose of this article is to give a comprehensive overview on both organisations' capabilities in cyber domain, highlighting main differences and common goals for them. Subsequently, a projection of further co-operation will be conducted. At the end, there will be recommendations for further joint cyberdefence involvement of NATO and the EU.

Comprehensive overview

The European Union has been working on cybersecurity issues since 2010 by creating, in 2013, Cybersecurity Strategy and the European Commission Initiatives towards cyberspace. Cybersecurity Strategy focuses on five main priorities: achieving cyber resilience, reducing cybercrimes, developing cyberdefence policy and capabilities related to Common Security and Defence Policy (CSDP), developing industrial and technological resources for cybersecurity, and establishing coherent international cybersecurity policy for the EU and promoting core EU values[1]. Each of these priorities addresses main European Union concerns related to cyberspace. By cyber resilience, the EU means "co-operation between public authorities and private sectors in providing security of the networks[2]". Because of this, the European Union has developed Network and Information Security policy – ultimately the NIS directive signed in 2015 – designed to enhance the level of shared knowledge regarding cyber incidents among public and private sector entities – between all Member States. To decrease the number of cybercrimes, the EU has focused, inter alia, on strong and effective legislation to tackle cybercrime[3], urge Member States to ratify

1 | http://europa.eu/rapid/press-release_IP-13-94_en.htm (access: 14.06.2016).

2 | European Commission Joint Communication from 7 February 2013 on cybersecurity JOIN(2013) 1 final, p. 5.

3 | European Commission Joint Communication from 7 February 2013 on cybersecurity JOIN(2013) 1 final, p. 9.

Budapest Convention on Cybercrime and support the European Cybercrime Centre (EC3). By developing cyberdefence policy and capabilities, the EU puts pressure on detection, response and recovery from cyberthreats[4]. By detection, response and recovery, the EU wanted to find synergies between civilian and military approaches, including "exploration possibilities on how the EU and NATO can complement their efforts to heighten the resilience of critical government, defence and other information infrastructures on which the members of both organisations depend[5]".

> By developing cyberdefence policy and capabilities, the EU puts pressure on detection, response and recovery from cyberthreats.

It was actually the first formal step in co-operation between the EU and NATO which led to an agreement in 2016[6]. The development of industrial and technological resources needed for better protection of cyberspace was the fourth of the EU Cybersecurity Strategy pillars. The European Union's focus was to provide common recommendations on how the cybersecurity questions should be present in value chain of the ICT products. One of the core ideas was to organise a Single Market for cybersecurity products within the EU and to support the development of security standards that should be respected by all actors of the ICT market. Finally, the EU deployed the need for coherent international cybersecurity policy for the EU. The European perspective contains three core values: openness and freedom in the Internet, and security of networks. This approach was developed and addressed in the EU external relations and Common Foreign and Security Policies.

Beyond the Cybersecurity Strategy (CSS), the European Commission was strengthening the engagement in cyberspace protection by the Cybersecurity Initiatives, which went along the CSS. The European Commission operated on four pillars: introduction of the EU Strategies related to cybersecurity (CSS, Digital Single Market Strategy, European Agenda on Cybersecurity), enhancement of the EU legislation (NIS Directive, Legislative frameworks to fight cybercrime), organisation of Platforms and Networks for co-operation (public-private on NIS, the EU Agency for Network and Information Security, the EU CERTs, Europol Cybercrime Centre (EC3)), and foundation of the three main cyber hubs: Cyber R&D, Digital Infrastructure and Capacity Building Engagements with third countries. Worth noticing is the fact of the EU involvement in international activities directed to establish dialogue and links with other international organisations, third countries and among Member States.

NATO's involvement in cybersecurity has started earlier than the European Union's. As a military alliance, NATO was far well aware of the threats and operations that materialised with geometrical increase of cyberthreats. Russian attack on Estonian government networks in 2007 was the accelerator for further NATO development in cyberdefence. In April 2008, NATO, as the first international organisation, announced Policy on Cyber Defence and shortly after signed documents to establish Cooperative Cyber Defence Centre of Excellence in Tallin. Then, in 2011, NATO Defence Ministers adopted new cyberdefence policy which comprised NATO's priorities and efforts to enable Member States further development of cyberdefence, including a call for international co-operation with other organisations like the EU. Between 2011 and 2016, NATO conducted series of meetings dedicated to further development and

4 | European Commission Joint Communication from 7 February 2013 on cybersecurity JOIN(2013) 1 final, p. 11.

5 | Ibidem.

6 | Logius, iEU seminar: Digitizing European GovServices [online] www.logius.nl/languages/english/ieu-seminar-digitizing-european-govservices-june-6th (access: 02.07.2016).

enhancement of NATO cyber capabilities meant to gain full operational readiness. In February 2016, NATO (NATO Computer Incident Response Capability) and the EU (Computer Emergency Response Team) signed a Technical Arrangement on Cyber Defence, to establish a formal way of sharing best practices and the exchange of information related to cyberdefence[7].
NATO Policy over cyber domain focuses on three assumptions: cyberdefence is part of Alliance's task of collective defence, international law applies to cyberspace and that Alliance should intensify the co-operation with the industry to provide new solutions for cyberdefence. Policy underlines also the need for further protection of NATO's and Member States' communication networks as a top priority for the Alliance.

Both organisations developed their cyber capabilities and although they are focusing on different approaches, there are still certain fields of co-operation that are and should be addressed by the EU and NATO authorities.

Common goals and main differences in development of cyber capabilities

As we asses both organisations' development, we are able to see main divergence between them. NATO focuses on cyberdefence of Alliance and Member States, while the EU puts more effort to enhance anti-crime cyberdefence and non-military cyber capabilities together with commercial interest in cybersecurity. Although there are differences between both organisations, we can still find common goals shared by them. The EU and NATO co-operation started in 2010 by joint staff-to-staff cyberdefence consultations and informal meetings. The EU was also observing NATO's annual cyberdefence exercises "Cyber Coalition." Previously mentioned Technical Arrangement signed between the European Union's CERT and NATO's NCIRC gave a formal framework of co-operation which now includes: advanced incident response co-operation by technical information exchange and best practices sharing. Both organisations have basic tools to enhance their cyberdefences but in a limited way. From the strategic perspective, the co-operation between them is crucial to ensure security in the cyberspace because most threats affect both military and civilian infrastructure. However, on a tactical level, there will always be a different approach in, for example, fighting against cybercrime and preparation of military task forces.

> "NATO, on its operational level, focuses on three dimensions: Assisting Individual States by supporting national authorities in securing infrastructure (Communication and Information Systems) used by the Alliance to conduct missions.

The EU is focusing on the operational level on the following issues: risk management, information exchange and incident co-operation (including incident reporting), ICT security research and innovation, collection and data analysis on emerging threats, promotion of risk management methods, and running pan-European exercises, as well as awareness rising and co-operation between different actors on the ICT market. It is also involved in the development of Europol's Cybercrime Centre (EC3) which serves as a hub of criminal information and intelligence database. The EC3 supports Member States in investigations, provides strategic analysis and supports training. All of these operational level initiatives are defensive measures which are dedicated to secure existing networks and critical infrastructure, and to address all civil threats that appear in the cyberspace.

7 | http://www.nato.int/cps/en/natohq/news_127836.htm (access: 14.06.2016).

NATO, on its operational level, focuses on three dimensions: Assisting Individual States by supporting national authorities in securing infrastructure (Communication and Information Systems) used by the Alliance to conduct missions. Support might have different shapes: exchange of information, sharing best practices or conducting exercises. The second level of NATO's engagement concerns development of cyber capabilities among which we can distinguish: NATO Computer Incident Response Capability which provides centralised and overall defence support to NATO's websites, implementation of definition of the targets for Allied countries on a national level, and NATO's Smart Defence Initiative which enables countries to work together to develop and maintain capabilities by using Malware Information Sharing Platform, Multinational Cyber Defence Capability Development project or Multinational Cyber Defence Education and Training. Except for defensive capabilities, NATO develops its offensive tools which are meant to be deterrence capabilities for the Alliance.

Further trends in co-operation

As cyberspace is a non-geographical reality constructed on open, vulnerable architecture with decentralised structure, we will always be facing more sophisticated attacks in the internet. There is a certain problem with definitions in cyberspace, while the virtual reality tends to be in a constant move. It will be very difficult to clearly distinguish military and non-military aggressions, thus it is clear that improved co-operation between international organisations like NATO and the EU will develop. As it comes to the EU and NATO, as long as both organisations are facing major threats posed on critical infrastructure, industry operational systems, websites protection and espionage, there will have to be a constant co-operation between them. However, on other fields – like electronic warfare capabilities, cyber tools dedicated to provide A2/AD capabilities for military purposes, or protection against mocking, stalking, personifications – each organisation will act separately. As it comes to operational level, both NATO and the EU will possibly expand partnership. Previous co-operation in exchanging information and sharing best practices is only an introduction to a solid and permanent partnership on: cyberthreats data basis, joint exercises, development of early warning capabilities, development of joint cyber facilities to train professionals, joint co-operation with non-military and non-state actors in securing networks, trainings for third parties, joint international efforts on diplomatic level to limit threats, and probably many other initiatives. The point is – further co-operation is indispensable.

“ While both organisations develop their cyberdefence agendas, new opportunities will appear to strengthen the co-operation between NATO and the EU on the operational level.

Recommendations

While both organisations develop their cyberdefence agendas, new opportunities will appear to strengthen the co-operation between NATO and the EU on the operational level. The EU will mostly focus on non-military protection, while NATO will further develop military network and military deterrence capabilities. On a certain level, both organisations will share some of their capabilities to better respond on appearing threats. To enhance both efforts in the cyberspace, the EU and NATO might consider the following steps:

1. Develop joint EU-NATO trainings.
2. Implement joint fighting botnet and malware platforms.
3. Expand joint NATO-EU cyber incident exercises.
4. Implement ongoing gap and vulnerabilities identification.
5. Match the capabilities that might be common

for further development, not to replicate them: doctrine, leadership, organisation, personnel, technology, infrastructure, logistics and interoperability.

6. Ensure joint dialogue with international organisations, other state and non-state actors to create common understanding for further international agreements regarding cyberdefence. ■

EUROPEAN CYBERSECURITY JOURNAL

SUBSCRIPTION AND ORDERING INFORMATION

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

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

PRICING OF THE ANNUAL SUBSCRIPTION (4 ISSUES)

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

Electronic edition: € 199
excluding VAT, including handling

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

CONTACT INFORMATION

The Kosciuszko Institute
editor@cybersecforum.eu
ul. Feldmana 4/9-10, 31-130 Kraków, Poland
Tel: +48.12.632.97.24

BANKING INFORMATION

Alior Bank
SWIFT: ALBPPLPW
IBAN: PL21 2490 0005 0000 4600 7451 5642

THE ECJ IS ADRESSED TO

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

FROM THE FOLLOWING SECTORS

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

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

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

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

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY JOURNAL