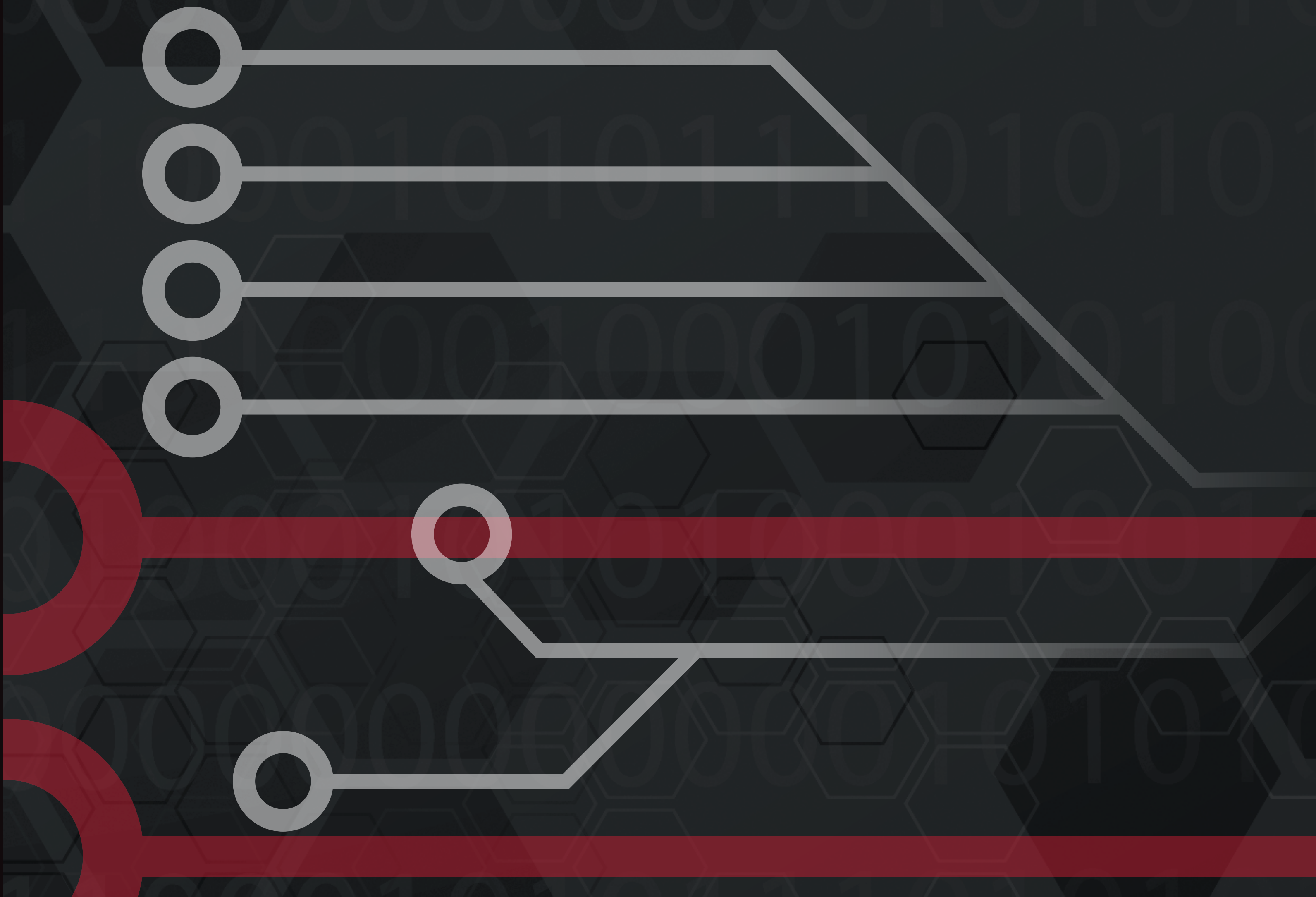
VOLUME 2 (2016) ▪ ISSUE 2

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES



ANALYSES ▪ POLICY REVIEWS ▪ OPINIONS

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY JOURNAL

VOLUME 2 (2016) ▪ ISSUE 2

EUROPEAN CYBERSECURITY JOURNAL

STRATEGIC PERSPECTIVES ON CYBERSECURITY MANAGEMENT AND PUBLIC POLICIES

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

EDITORIAL BOARD

ISSN: 2450-21113

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 2, page reference

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

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

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

Printed in Poland
by Drukarnia Diament | diamentdruk.pl

DTP: Marcin Oroń

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

EDITORIAL

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

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

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

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

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

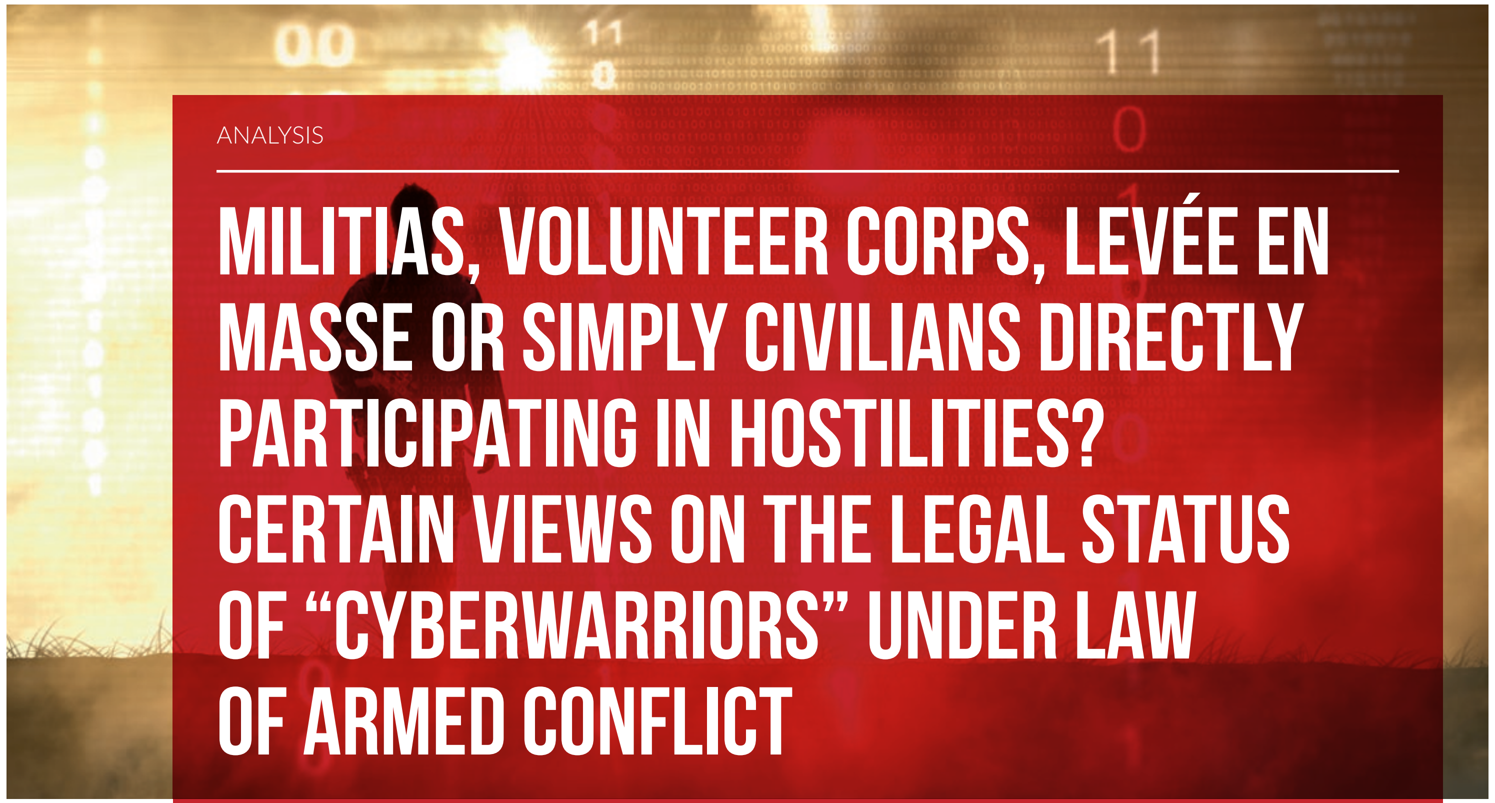
In the process, we have decided to include all key stakeholders: representatives of public entities, business leaders, experts, scientists, and representatives of the civil society. Bringing together so many diverse points of view is our core value. It also makes us stand out when compared to other projects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

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

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

Joanna Świątkowska

CONTENTS



ANALYSIS

MILITIAS, VOLUNTEER CORPS, LEVÉE EN MASSE OR SIMPLY CIVILIANS DIRECTLY PARTICIPATING IN HOSTILITIES? CERTAIN VIEWS ON THE LEGAL STATUS OF “CYBERWARRIORS” UNDER LAW OF ARMED CONFLICT

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

1. Introduction

Growing „civilianisation" of contemporary armed conflicts is a fact. More and more civilians are present on or in vicinity of battlefields all over the world. Significant share of what used to be traditional military functions is nowadays being outsourced. This is caused mainly by two factors: gradual personnel reductions in most of the armies and growing reliance of the militaries on modern technology. Civilians (sometimes contractors) are hired to perform multiple functions from catering and logistics, through force protection, to providing actual combat force on the battlefield. Nowadays, it is not unusual to see civilian specialists operating or maintaining military equipment, weapon systems etc. for which highly specific knowledge, skillset and experience are required that the military lacks.

It is no secret that most militaries lack the expertise in cyberarea, thus it is highly likely that civilian specialists (most probably contractors) would become the “first choice cyberwarriors.” Also, because cyber operations are relatively inexpensive, they may be considered particularly attractive by non-state actors engaged in asymmetric conflicts or hybrid warfare. Depending on multiple factors, such as the type of conflict, affiliation to state or non-state party, the nature of the relationship with the party to the conflict, the status of “cyberwarriors” under the law of armed conflict (LOAC) may vary. The purpose of this short article is to shed some light on the complicated, yet fascinating issue of the status of persons engaged in cyberwarfare and implications thereof. For the purpose of this article, let us assume that cyberwarfare is either used in a broader armed conflict or independent cyber operations amount to armed attacks, thus trigger the initiation of an armed conflict.

Firstly, we will examine the matter of if and how Law of Armed Conflict (LOAC) applies to cyber hostilities (or cyberwarfare). Then, we will consider how the principal combatancy criteria as set forth in Geneva Convention 3 and Additional Protocol 1 to Geneva Conventions can be used in relation to "cyberwarriors." Next, the notion of direct participation in hostilities and organised armed groups will be assessed in the cyber context to culminate in an analysis of different possible options for legal status of persons involved in the conduct of cyber hostilities.

2. Applicability of LOAC to Cyberwarfare

There should be no doubt that international law applies to cyberspace and operations conducted therein. It has been recognised by the North Atlantic Treaty Organisation (NATO) in its Wales Summit Declaration[1] and confirmed by many scholars and legal experts, to include the drafters of the Tallinn Manual[2].

Undoubtedly, LOAC applies whenever an armed conflict exists, regardless of whether parties to the conflict recognise its existence and regardless of whether the conflict is of international or non-international character, as provided for in Articles 2 and 3 common to the four Geneva Conventions. From that perspective, if cyberactions cross the threshold of an armed attack, even if hostilities occurred only in cyberspace, without resort to conventional (or rather – traditional) means and methods of warfare, there will be an armed conflict, entailing the application of LOAC[3]. Modern means and methods of warfare do not evolve in a legal vacuum. Neither does legal vacuum exist in cyberspace[4]. To that end, it is worthwhile to quote the so called Martens Clause:

"Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience[5]."

More recently, the Martens Clause was restated in Additional Protocol I, Art. 1(2): *"Recalling that, in cases not covered by the law in force, the human person remains under the protection of the principles of humanity and the dictates of the public conscience."*

In its commentary, the ICRC states that although the Martens Clause is considered to be part of customary international law[6], the plenipotentiaries considered its inclusion appropriate because:

"First, despite the considerable increase in the number of subjects covered by the law of armed conflicts, and despite the detail of its codification, it is not possible for any codification to be complete at any given moment; thus the Martens clause prevents the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted. Secondly, it should be seen as a dynamic factor proclaiming the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology[7]."

Nowadays, the international community observes rapid development in military technology and also the means and methods of warfare. It is enough to mention the so called hybrid warfare, *"internationalised non-international armed conflicts"* (e.g. ISAF), development of autonomous weapon systems and, last but not least, the growing interest in examining the potential of offensive application of cybermeans and methods of warfare.

> "Apparently, there should be no doubt about LOAC applicability to cyberwarfare. The question is rather how LOAC applies to cyberwarfare, in particular whether (or when) it could be applied directly, or is there a need for mutatis mutandis application.

Drafting and adopting LOAC treaties obviously cannot keep the pace with technological and doctrinal developments in the area of modern warfare, thus the Martens Clause provides a "safety switch," recognised as customary international law that requires – should everything else fail – at least the application of the core four LOAC principles to all and any types of hostilities or means and methods of warfare.

In the author's view, this doesn't mean that only the core principles of LOAC apply to cyberwarfare. It just means that there can be no excuse to non-compliance with at least the core principles, even if it is recognised that there is no specific LOAC provisions governing for instance cyberwarfare, as opposed to explicit LOAC provisions restricting or prohibiting the use of certain conventional weapons, such as incendiary weapons, booby traps, laser weapons or expanding bullets.

Apparently, there should be no doubt about LOAC applicability to cyberwarfare. The question is rather how LOAC applies to cyberwarfare, in particular whether (or when) it could be applied directly, or is there a need for *mutatis mutandis* application. In the following section, this question will be answered with the example of combatancy criteria, as applicable to conduct of hostilities in cyberspace.

3. Cyberwarriors as Combatants

There is no simple definition of combatant. In fact, a number of IHL instruments contain different definitions of combatants. All of them are consistent when it comes to the obvious: granting combatant status to armed forces belonging to the party to the conflict. Differences (although perhaps not fundamental) occur with regards to other groups, militias, etc. belonging to the party to the conflict. Let us, however, start with defining the notion of armed forces.

Additional Protocol I to Geneva Conventions in its Article 43(2) provides perhaps the most comprehensive and widely adopted definition which states: *"The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which,*

[1] Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, visited 18 January 2016.

[2] Tallinn Manual on the International Law Applicable to Cyber Warfare, general editor Michael N. Schmitt, Oxford University Press, 2013, p. 13.

[3] Knut Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks: an ICRC Approach' in Karin Byström (ed.) International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference (Stockholm: Swedish National Defence College, 2004), 142-143, http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, visited 24 Jan 2016.

[4] No legal vacuum in cyber space, 16-08-2011 Interview with Cordula Droege, ICRC legal adviser, https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, visited 31 Jan 2016.

[5] Preamble to the Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, https://www.icrc.org/applic/ihl/ihl.nsf/ART/195-200001?OpenDocument, visited 31 Jan 2016.

[6] Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, p. 39, https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=7125D4CBD57A70DDC12563CD0042F793 visited 03 Feb 2016.

[7] Ibidem, pp 38-39.

inter alia, shall enforce compliance with the rules of international law applicable in armed conflict." Militias and volunteer corps, if incorporated into the armed forces, are subject to the same requirements, as applicable to regular armed forces. It should be noted, however, that the legal regime and criteria governing membership or incorporation into the armed forces are generally contained in national legislation.

Members of other (i.e. those not forming part of armed forces) militias, volunteer corps, organised resistance movements, *levée en masse* can also be recognised as combatants, given they fulfil certain criteria that armed forces are considered to fulfil *ex lege*[8]. These criteria are formulated differently in Additional Protocol I, Geneva Convention III and the so called Hague Regulations[9], however can be reduced to the following:

1) being commanded by a person responsible for his subordinates;
2) having a fixed distinctive sign visible at a distance;
3) carrying arms openly;
4) conducting operations in accordance with the laws and customs of war.

If the four aforementioned criteria are fulfilled cumulatively, even members of irregular formations that do not constitute parts of armed forces, yet take part in hostilities, can enjoy the benefits of combatant status, to include combatant immunity, i.e. *"they shall not be called to account for their participation in lawful military operations*[10]*"* and should be granted prisoner of war status upon capture.

As criteria number one and four are rather uncontroversial (even in computer network operations), at least with regard to regular armed forces (who, by the way, will also always fulfil the requirement of *"belonging to a party to the conflict,"* thus simplify the issue of attribution if a cyberattack is conducted by members of regular armed forces), let us stop for a moment to analyse number 2 and 4 as crucial for compliance with the principle of distinction (between combatants as lawful military objective and civilians by default protected from attacks) and the obligation for combatants to distinguish themselves from civilians. Additional Protocol 1, Article 44(3) requires combatants to have a distinctive sign and carry arms openly while they are engaged in an attack or in a military operation preparatory to an attack. Yet, recognising certain specificities of guerrilla warfare, where "[...] *owing to the nature of the hostilities an armed combatant cannot so distinguish himself* [...]," AP I provides that "[...] [such armed fighter] *shall retain his status as a combatant, provided that, in such situations, he carries his arms openly*:

a) during each military engagement, and
b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate."

The reason for enforcing the obligation for belligerents to distinguish themselves from civilians is the obligation to protect civilians from direct attack, *"unless and for such time as they take a direct part in hostilities."* As will be discussed in more detail in the following section, the possibility to consider civilians as lawful military objectives is normally "conduct-based" (if they take direct part in hostilities), except for members of organised armed groups, who – similarly to members of armed forces – can be targeted by virtue of their status as members[11].

Today, modern means and methods allow remote conduct of hostilities. Computer network operations or cyberattacks are no different to that end from unmanned combat aerial vehicles (UCAVs) or stand-off weapons, that significantly reduce the prosper of capture of the person engaged in attack with the use of cybermeans, UCAV or stand-off weapons, yet make the attackers practically invisible to the enemy in the course of an attack. This makes some of the scholars to consider the four criteria less relevant for cyberwarriors than "conventional fighters," as opposed to the requirement to belong to a party to the conflict[12].

If a cyberattack is conducted by an entity that does not form a part of the armed forces, the issue of affiliation to a party to the conflict becomes somewhat challenging. Any governmental institution meets the requirement of belonging to a party to the conflict, but it is not so clear with respect to e.g. private enterprise, to which a state has turned to have carried out a network attack because of their knowledge, skills and technical capabilities. The requirement of affiliation may be met through a factual relationship, functional, which does not need to be formalised, but if such a link actually exists (e.g. in the form of a contract), it should be considered as satisfying the requirement of belonging to a party to the conflict.

Affiliation with a party to the conflict also involves state responsibility for the actions of armed groups carried out "at the request" of the state. One of the key principles of international law is that states (rather than individuals) bear liability for violation of obligations under international binding upon that state, if the breach is a consequence of actions that can be attributed to that state. State will bear the responsibility for the actions of their bodies and government institutions (including the armed forces) that constitute violations of international law, but would also be liable for the actions of private actors by order of state authorities, in accordance with the instructions of the state bodies under the direction or control of the State (criterion of effective control as in the case of *de facto* commanders)[13]. The principle applies to all military operations, conducted both by the regular armed forces and other organised groups meeting the criteria of Art. 43 of the first Additional Protocol, but is of particular importance in the context of operations in cyberspace that would be outsourced to private entities.

> " Affiliation with a party to the conflict also involves state responsibility for the actions of armed groups carried out "at the request" of the state.

Even if the cyberattack qualifies as armed attack, that is, it is reasonable to assume that it would result in injuries to or death of persons or damage to or destruction of buildings, in most cases, such an attack will be carried out from a remote location, without direct contact between the attacker and the attacked. This may suggest that the requirement for combatants conducting a network attack to distinguish themselves from civilians by wearing fixed distinctive signs becomes less relevant,

[8] | Leslie C. Green, The Contemporary Law of Armed Conflict, Juris Publishing, Manchester University Press, Manchester 2000, pp. 34-35; Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law. Volume I: Rules., International Committee of the Red Cross, Cambridge University Press, Cambridge 2005, pp. 15-16.

[9] | Regulations Respecting the Laws and Customs of War on Land annexed to Convention (IV) respecting the Laws and Customs of War, The Hague, 18 October 1907, https://www.icrc.org/ihl/INTRO/195 access 14 February 2016.

[10] | Knut Ipsen, Combatants and non-combatants in: The Handbook of International Humanitarian Law, edited by Dieter Fleck, Oxford University Press, Oxford 2009, p. 95.

[11] | Sean Watts, Combatant Status and Computer Network Attack, in: Virginia Journal of International Law, Vol. 50 – Issue 2, Virginia Journal of International Law Association, 2010, p. 420; Of note, even being considered a member of an organized armed group does not automatically entail combatant privileges or combatant immunity if the four combatant criteria prescribed above are not met.

[12] | Ibidem, pp. 337-441.

[13] | Guenael Mettraux, The Law of Command Reposnsibility, Oxford University Press, Oxford 2009, s. 100-102, 110-113, 122-123.

especially in situations in which the network attack is carried from within a military objective, for which there is a separate obligation to mark it (e.g. a warship or military aircraft)[14]. Nevertheless, in the author's view, the distinction requirement can be met by e.g. using IP addresses that are clearly different from those used by civilians or civilian entities or at least – when hiding the IP address from the objective of the cyberattack (as a mean to avoid or hamper counteractions) – using such tools that are specific to the military and leave no room for allegations of feigning civilian status which would be considered as perfidy in accordance with AP I Art. 37(1).c[15].

Similar approach could be adopted with regards to the criterion of carrying arms openly. Conventional (or "classical") weapons are not used in computer network operations. It would be hardware or software, both either specifically developed or adjusted to carry out cyberattacks. As it is difficult to expect "cyberwarriors" to carry their laptops marked as weapons with special stickers, especially if they are sitting thousands of miles away from their targets, perhaps the use of specific malware, not available "off the shelf" to any "hacker wannabe," or "weaponised" software clearly distinct from its civilian analogues, is the vehicle to ensure the weapons carrying criterion is met, except for cyber *levée en masse* (to be discussed in more detail in Section 5 of this article), for which spontaneous "taking up arms" might prevent the possibility to obtain militarised or weaponised information technology (hardware or software), but which – arguably – cannot exist in borderless cyberconflicts[16].

4. Direct Participation in Hostilities (DPH) and Organised Armed Groups (OAGs) in the Cyber Context

Additional Protocol 1 Art. 51.(3) and Additional Protocol 2 Article 13.(3) provide that civilians are immune from direct attack unless and for such time as they take a direct part in hostilities. They lose this protection for the duration of each act amounting to direct participation, however, this conduct-based concept should only apply to civilians who are neither members of armed forces (to include militias and volunteer corps incorporated into the armed forces) or organised groups nor participate in *levée en masse*. For members, their membership alone is sufficient to determine their status as lawful military objectives (although criteria of membership will differ, as will be discussed below), regardless of whether they actually take direct part in hostilities at a given time. In an effort to define both the notion of DPH as well as membership in organised armed groups, International Committee of the Red Cross (ICRC) has issued its guidance[17] which, in fact, was the first comprehensive study on this topic. Although controversial in many aspects[18], it actually provides good overview of the issue and served as a catalyst for in-depth discussions of the practicalities of the DPH concept and its application in contemporary armed conflicts, most of which has been asymmetric over the last two decades.

a) DPH Criteria

What are the cumulative criteria that an act has to fulfil in order to be considered as amounting to DPH? In accordance with the ICRC guidance, these are: 1) threshold of harm, 2) direct causation and 3) belligerent nexus.

1) **Threshold of harm** – the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack. Acting to the benefit of one's own party to the conflict the act has to result or be likely to result in negative consequences to the enemy's military effort[19]. It should be noted that adversely affecting military operations or capacity of the other party does not necessarily require causing physical damage. The ICRC guidance states that "[e]*lectronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE).*"

2) **Direct causation** – there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part. For example, transporting weapons or other military equipment may be considered to be directly related to cause harm in military terms (and thus constitute DPH) only when it is executed as an integral part of a specific military operation, planned to inflict appropriate amount of damage (of sufficient degree of harm). Therefore, training or recruiting militants for organised armed groups, although it is essential to the military capabilities of the group, will not fulfil the direct causation criterion, unless it will be carried out in order to prepare a pre-planned specific military operation or hostile act. In this case, because the training or recruitment might be considered an integral part of the operation, and the causal link to the operation will be direct[20]. The guidance recognises that CNAs, despite their remoteness, will in most cases meet the direct causation test[21].

3) **Belligerent nexus** – an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (carried out to gain definite military advantage). From that perspective, organised self-defence of the civilian populace against pillaging or other acts of violence towards the populace, even if resulting in hostile acts against the party to the conflict that fulfil the other two criteria, shall not be considered as DPH. Similarly, bank robbery (to include "cyber-robbery") committed by belligerents for their personal gain (not in support of the military operation of a party to the conflict) should be considered a criminal act rather than DPH[22].

The ICRC Guidance does not provide many examples of acts amounting to DPH in the cyber context. Nevertheless, if a cyberattack can amount to an armed attack, certain activities conducted in or through cyberspace will definitely fulfil criteria of direct participation in hostilities. The following three examples might be useful to illustrate the concept of DPH in the cyber domain.

Scholars tend to agree that designing malware (even for military purposes) would usually not fulfil the three criteria of DPH, unless such malware is specifically designed to exploit vulnerabilities of particular target or modified (customised) to be used in a specific cyberattack[23].

[14] | Tallinn Manual, op. cit., pp. 99-100.

[15] | Sean Watts, op. cit., p.442; see also Vijay M. Padmanabhan, Cyber Warriors and the Jus in Bello in: International Law Studies vol. 89 (2013), U.S. Naval War College, 2013, pp. 295-296.

[16] | David Wallace, Shane R. Reeves, The Law of Armed Conflict's "Wicked" Problem: Levée en Masse in Cyber Warfare, in: International Law Studies vol. 89, op. cit, pp. 662-663.

[17] | Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, International Committee of the Red Cross, Geneva 2009.

[18] | See e.g. Michael Schmitt., The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis in: Harvard National Security Journal Vol. 1, May 5, Cambridge (Massachusetts) 2010; Kenneth Watkin, Opportunity Lost: Organised Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance, in: New York University School of Law Journal of International Law and Politics Vol. 42, No. 3, New York 2010.

[19] | Nils Melcer, op. cit., p. 47.

[20] | Ibidem, p. 53. An example of training or recruitment that meets the direct causation test might be to select volunteers to conduct suicidal IED attack, and to train them on the topography of the object of attack, infiltration methods and vulnerabilities to be exploited in order to successfully execute the attack.

[21] | Ibidem, p. 55.

[22] | Ibidem, p. 62-63.

[23] | Hanneke Piters, Cyber Warfare and the Concept of Direct Participation in Hostilities, in: NATO Legal Gazette Issue 35 (December 2014), p. 54, http://www.act.nato.int/images/stories/media/doclibrary/

Installation, servicing and maintenance of computer systems or software would normally not amount to DPH, especially if linked to passive (or reactive) cyberdefence. If, however, the system (or software) in question is being installed in preparation for launching a cyberattack at a specific target, it would amount to DPH, because "[measures] *preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution, constitute an integral part of that act.*[24]"

Lastly, operation of a computer system or software in the course of a cyberattack (fulfilling the criteria of an armed attack, as assumed in the beginning of this article) would in most cases amount to DPH, regardless of whether the malware is to activate instantly or contains "delayed fuse" designed so that the malware took intended effects at a given point in time[25]. Exploring general vulnerabilities in software operated by the enemy would not amount to DPH, as opposed to exploiting such vulnerabilities in preparations for a cyberattack or in support of a conventional attack, just as collecting tactical intelligence would be considered DPH, whereas strategic intelligence activities would not[26].

b) Organised Armed Groups (OAGs)

Considerations on the subject of organised armed groups should be started with a statement that the concept of organised armed groups (OAGs) functions only in non-international armed conflicts (NIACs), where the state party to the conflict is represented by governmental security forces (to include regular armed forces) and the non-state party is fought for by either dissident armed forces (mutinied part of the armed forces) or OAGs. As the legal notion of combatants cannot be referred to with regard to persons engaged in hostilities on the non-state party to the conflict, the term "fighters" that encompasses both members of dissident armed forces and OAGs is being used despite not being reflected in LOAC treaties[27].

It should also be noted that in accordance with Article 3 common to all four Geneva conventions, applicability of Geneva conventions to NIAC is very limited, therefore provisions of Geneva Convention III (relative to the Treatment of Prisoners of War) dealing with combatancy and POW status will not apply, unless parties to the NIAC "[...] *bring into force, by means of special agreements, all or part of the other provisions* [...]" of the Convention. Neither will provisions of Additional Protocol I apply and thus there are no combatants or POWs in NIACs, although enemy fighters will constitute lawful military objectives.
As opposed to civilians who sporadically or spontaneously take direct part in hostilities and are considered "fighters" for the duration of each act amounting to DPH[28], persons who qualify as members of OAGs, become lawful military objectives for the duration of their membership, allegedly in a manner similar to members of regular armed forces. This means that as long as the membership exists, these persons can be targetable 24/7.

OAGs should belong to the non-state to the conflict (and the belonging could in fact mean even loose linkage materialised in following the directions and guidance of the non-state party) and fulfil the criteria laid down in Article 1(1) of Additional Protocol II, namely being under responsible command and exercising "[...] *such control over a part of [the state party's] territory as to enable them to carry out sustained and concerted military operations and to implement* [Additional Protocol II]." Putting aside the problematic question of territory in cyberspace, let's simplify the issue by adopting an assumption that there is an OAG fulfilling the aforementioned criteria and focus on the membership issue.

Membership in OAGs shall not be linked to a formalised joining or recruitment. There will be no formal relationship or bond, no formalised and common uniforms with distinctive signs and no identification cards serving the purposes of Geneva Convention III. In accordance with the ICRC Guidance, the only determining factor will be the so called continuous combat function constituting the foundation of the functional relationship with an OAG. Assumption of this continuous combat function is to be the objective indication of membership.

ICRC stated that continuous combat function requires lasting integration with an OAG and usually this function would be to take direct part in hostilities, although persons whose functions involve preparing, conducting or commanding operations or actions amounting to DPH is believed to have had continuous combat function. Persons, who within an OAG fulfil non-combat functions (administrative, political, logistic), in accordance with the ICRC guidance should not be considered members of that OAG, which has become a point of friction, as – in the opinions of some of the experts – it results in unequal treatment of regular armed forces and OAGs[29].

Also, a person who has been recruited, trained and equipped by an OAG to repeatedly take direct part in hostilities may be considered a member of this OAG (and thus a lawful military objective that may be subject of lethal targeting) even before committing the first act amounting to DPH, if upon completion of the training the person concerned does not "leave" the OAG. This is one more example of controversies behind the ICRC guidance: if there is no formalised joining criteria, how is it possible to determine if resignation took place?

Shifting to the cyberwarfare context, if the ICRC guidance was taken into account literally, only persons who joined an OAG in order to conduct cyberattacks crossing the threshold of armed attacks or in other manner amounting to DPH as illustrated above could be considered members and thus targetable throughout the duration of their membership (however the duration could be determined). Other persons affiliated with a cyber-OAG could only be targeted for the duration of each act amounting to DPH. Enjoying immunity from direct attack in military terms does not preclude facing criminal liability, though, as even Additional Protocol II, art. 6.(5) seems to recognise that taking part in a NIAC would violate criminal laws of the state party to the conflict and – as opposed to members of armed forces belonging to the state party – fighters on the non-state side would not enjoy combatant immunity.

From that perspective, hacktivists would normally face penal consequences of their actions, however members of hacker groups trained to conduct cyberattacks amounting to DPH or crossing the threshold of armed attack would fall within the category of lawful military objectives, whose *"partial or total destruction, capture or neutralisation"* would be lawful, if offering a definite military advantage in the circumstances ruling at the time[30].

5. Concluding Remarks – Lawful Options for Cyberwarrior Formations

A natural conclusion can be drawn from the considerations above: the optimal solution for cyberwarriors is to be members of the armed forces of a party to the conflict and there are

legal_gazette_35.pdf, access 16 February 2016.

[24] | Nils Melzer, op. cit, p.17.

[25] | Hanneke Piters, op. cit., pp. 55-56.

[26] | Ibidem, pp. 34-35, 49, 52, 66-67.

[27] | Michael N. Schmitt, Charles H.B. Garraway, Yoram Dinstein, The manual on the Law of Non-International Armed Conflict with Commentary, Martinus Nijhoff Publishers, Leiden/Boston 2006, pp. 4-5.

[28] | This is one of the biggest controversies behind the ICRC Guidance, referred to by some scholars as the "revolving door concept" allowing fighters to regain protected civilian status after committing DPH, perfectly captured in the phrease "farmer by day, fighter by night". See e.g. Kenneth Watkin, Opportunity lost..., op. cit. pp. 686-690.

[29] | Michael Schmitt, The Interpretive Guidance..., op. cit., pp. 15, 22-23.

[30] | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 29.

several nations who have stood up their military organisations or units to deal with cyber operations (both defensive and offensive). Examples include U.S. Cyber Command (CYBERCOM), Chinese People's Liberation Army General Staff 3rd Department and Unit 61398, Israeli Defence Forces Unit 8200 or Democratic People's Republic of Korea Bureau 121[31].

> “ the optimal solution for cyberwarriors is to be members of the armed forces of a party to the conflict

Members of armed forces are combatants, they are entitled to participate in hostilities and they enjoy combatant immunity for their actions in the course of hostilities, as long as these actions do not violate LOAC. Combatant immunity is of particular importance to those, who engage in offensive cyber operations or such cyberdefence activities that could be considered *"acts of violence against the enemy"*, as provided for in Article 49(1) of Additional Protocol I.

However, is it only military units and their personnel wearing uniforms that constitute armed forces? No, because as provided for in Article 43(1) of Additional Protocol 1, "[t]*he armed forces of a party to the conflict consist of all organised armed forces, groups and units which are under a command responsible to that party for the conduct of its subordinates*." The quoted provision is considered a reflection of customary international law, which state practice has confirmed over decades and is equally applicable to international and non-international armed conflicts. In countries where militia or volunteer corps (so-called "irregular" armed forces) constitute the army, or form part of it, they are included under the denomination "army". This definition is also used in Article 4 of the Third Geneva Convention, with the addition of organised resistance movements. Yet, with the privileges of combatant immunity and the right to engage in hostilities, come the obligations for the non-regular parts of the armed forces (i.e. militias, volunteer corps and organised resistance movements) to fulfil the four criteria of combatancy, as described in Section 3 above. It also requires incorporation into the armed forces that would enable the enforcement of command and control and disciplinary regime that ensures compliance with LOAC. The same requirement incorporation pertains to paramilitary organisations or armed law enforcement agencies that for the duration of an armed conflict may become parts of the armed forces (e.g. U.S. Coast Guard or Polish Border Guards).

Such incorporation would usually require a formal act, for example, an act of parliament that would define the membership criteria and requirements in a manner similar to the military. In the absence of formal incorporation, the status of such groups could be based on the facts and in the light of the criteria for defining armed forces[32].

This incorporation is a perfect vehicle to make voluntary defence organisations (defence leagues) specialised in cyberdefence or cyberwarfare more generally, comprised of talented specialists working as civilians on a daily basis, but undertaking certain military training similar to reservists, to fall under the protective umbrella of combatant status, should an armed conflict occur. Such cyber specialists wouldn't need to be mobilised as regular reservists, but the defence organisation to which they belong could be incorporated into the armed forces as a whole, with its organisational structure, personnel and equipment. Additional Protocol I requires a party to the conflict to notify such incorporation to the other parties to the conflict.

It is obvious that vast majority of expertise in cyber (defence) lies with the private (or civilian) sector. Some nations' militaries didn't develop their organic cyber capabilities, not to mention forming cyber-specialised units. Some nations, due to regulatory restrictions, cannot offer their uniformed personnel performing cyber duties emoluments that would be more attractive than those paid by big corporations, however they can either hire civilian employees or outsource such capabilities from the private sector, as the military does in many other areas previously belonging to the military (e.g. logistics). What would be the legal status of such civilian employees or contractors under LOAC?

Both civilians accompanying the force and contractors do not form part of the armed forces[33]. And though as a general rule, they are immune from direct attack, they share the risks and dangers of war alongside with the armed forces they accompany[34]. The ICRC Guidance provides that "[p]*rivate contractors and employees of a party to an armed conflict who are civilians* [...] *are entitled to protection against direct attack unless and for such time as they take a direct part in hostilities. Their activities or location may, however, expose them to an increased risk of incidental death or injury even if they do not take a direct part in hostilities*."[35] If, however, civilians are employed or contractors outsourced to perform combat function that fulfils DPH criteria, to include cyberattacks, they lose their protection from attack without gaining combatant privileges.

Moreover, in certain circumstances, as defined in Additional Protocol I, Art. 47(2)[36], civilian employees or contractors performing combat functions (taking direct part in hostilities, engaged in warfare), may be considered as mercenaries, especially if their wages in order to be competitive compared to those offered by private sector are significantly higher than those paid to the military. Persons determined mercenaries are not entitled to combatant privileges and thus – if captured – do not enjoy POW status and may be prosecuted for not only taking direct part in hostilities, but also for the fact of being mercenaries, which is penalised by many national criminal legislations.

With regard to other types of formations that may be considered combatants under LOAC, basically all of them raise significant questions to their applicability in the cyber context. Firstly, *levée en masse* defined as "*the inhabitants of a country which has not yet been occupied who, on the approach of the enemy, spontaneously take up arms to resist the invading troops without having time to form themselves into an armed force.*" Although – as stated by some scholars[37] – due to the nature of cyberconflicts (no borders and no territories) – *levée en masse* would not exist in such conflicts, one could imagine spontaneous creation of a cyber *levée en masse* in reaction to an enemy invasion. It does, however raise an issue of carrying arms openly. Even the solution mentioned above, i.e. utilising unique IP addresses or non-civilian technologies to conceal the IP addresses, might be problematic, as it is impossible for the military to share the technologies with a spontaneously emerging group. Yet, there might be options for cyber *levée en masse* to distinguish themselves from civilian network users, by e.g. publically announcing that certain

[31] | Paul Walker, Organizing for Cyberspace Operations: Selected Issues, in: International Law Studies vol. 89, op. cit., pp. 342-343.

[32] | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 17.

[33] | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 13.

[34] | Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare, ed. by Yoram Dinstein and Bruno Demeyere, Program on Humanitarian Policy and Conflict Research at Harvard University, Version 2.1, Harvard University, Cambridge (Massachusetts) 2010, pp. 270-271.

[35] | Nils Melzer, op. cit., p. 37.

[36] | A mercenary is a person who: 1) is specially recruited locally or abroad in order to fight in an armed conflict; 2) does, in fact, take a direct part in the hostilities; 3) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; 4) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; 5) is not a member of the armed forces of a Party to the conflict; and 6) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

[37] | See supra note 16.

sources of cyber actions or certain cyber tools are used solely by that cyber *levée en masse*.

Similar issues arise with other irregular groups: other (i.e. not belonging to nor incorporated into armed forces of a party to the conflict) militias and volunteer corps and organised resistance movements. As opposed to *levée en masse*, they are required to fulfil all the four combatancy criteria, as it assumes that they have sufficient time for organising themselves in a manner allowing to develop responsible command and disciplinary regime enabling to enforce compliance with LOAC, however fulfilment of the requirement to carry arms openly may become equally problematic without access to typically military cyber technologies.

6. Summary and a handful of recommendations

Full compliance with LOAC requirement in cyberwarfare might be challenging even for regular armed forces, which by definition are supposed to e.g. fulfil all the combatancy criteria. It gets even more challenging for irregular fighting groups, as hopefully has been proven above. Challenging doesn't mean impossible, though, and LOAC itself comes with assistance offered by the Martens Clause encouraging flexible approach to certain LOAC provisions. Adaptability of LOAC is its great advantage and – as stressed in recommendations from the First European Cybersecurity Forum – CYBERSEC.EU 2015, "[...] *legal framework governing the conduct of hostilities in cyberspace is sufficient* [...] *and the tendency to over-regulate should be avoided*[38]."

There are two principal ways of ensuring that "cyberwarriors" lawfully engage in hostilities: enrolment to the armed forces or becoming member of a militia or voluntary corps that complies with LOAC criteria of combatancy. One of the recommendations from CYBERSEC.EU 2015 was establishment of voluntary civic defence leagues composed of skilful and talented individuals capable of employing cybermeans and methods of warfare effectively. In order for such defence leagues to be entitled to lawfully take part in hostilities they could be either:

1) Offered and accepted up front to be incorporated into the armed forces upon commencement of an armed conflict; such defence leagues would have to lobby for their governments to introduce appropriate legislation (preferably before, not after the conflict has started); should circumstances require, military cyber technologies could be made available in advance to such civic defence leagues (to include appropriate training); or

2) If not incorporated into the armed forces, they would have to ensure on their own that they meet all the combatancy criteria; this might be more challenging, especially without access to military technologies clearly distinct from cybermeans and capabilities available to "regular" civilians.

> " There are two principal ways of ensuring that "cyberwarriors" lawfully engage in hostilities: enrolment to the armed forces or becoming member of a militia or voluntary corps that complies with LOAC criteria of combatancy.

The former option – although initially more formalised and requiring adoption of respective legislation – offers subsequent simplicity in implementation and execution, as well as full compliance with LOAC requirements and perhaps this is the option that should be pursued in order to enable talented individuals who are civilians in their regular life to become lawful cyberwarriors, should homeland call to arms. ■

[38] CYBERSEC 2015 Recommendations, p. 11, https://app.box.com/s/kb6zaq06v0uyhdh7pr13zk132uiwvu2u, access 21 February 2016.

OPINION

HACKERS, HACKTIVISTS, AND THE FIGHT FOR HUMAN RIGHTS IN CYBERSECURITY

STEFANIA MILAN
Stefania Milan (stefaniamilan.net) is an assistant professor at the University of Amsterdam and the Principal Investigator of the DATACTIVE project, exploring the politics of massive data collection (European Research Council Starting Grant 639379). She is also a research associate at the Tilburg Institute for Law, Technology and Society (Tilburg University) and at the Internet Policy Observatory of Annenberg School of Communication (University of Pennsylvania). Her research explores cyberspace and cybersecurity governance, grassroots engagement with technology and data epistemologies. Stefania is the author of Social Movements and Their Technologies: Wiring Social Change (Palgrave Macmillan, 2013) and co-author of Media/Society (Sage, 2011).

1. Introduction

Edward Snowden, the US security contractor turned whistleblower, has exposed blanket data surveillance programs targeting citizens indiscriminately, regardless of their criminal record or passport. The current surveillance complex combines the state apparatus and the industry in unprecedented tight alliances, largely hidden to users and generally impermeable to democratic safeguards[1]. In the same year, the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, has denounced threats this surveillance frenzy represent for human rights. He argued that 'Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy, and threatens the foundations of a democracy society. He exposed, among others, the unregulated access to communications data, the lack of judicial oversight over massive data collection, the mandatory data retention requirements imposed on manufacturers and providers of electronic communication, the extra territorial application of surveillance laws and the extra-legal surveillance[2]. But if a variety of non-governmental organisations has made their voice heard, and the use of encryption is on the rise, the bulk of the citizenry ignores that their civic rights are progressively being eroded in the name of underspecified cybersecurity needs, spanning anything from the fight against global terrorism to the curbing of copyright infringement. Cybersecurity policymaking remains, to a large extent, a grey area which is exclusive to security agencies, top-level technocrats and the military. The state-industry alliance is rarely broken, and only when the manufacturers of the 'tethered' devices[3] that constitute the final link in the chain of surveillance publicly stand up against law enforcement requests, as the recent Federal Bureau of Investigations vs. Apple case shows[4]. But while from the perspective of the state the imperatives of national security are perfectly legitimate and dutiful, there remain some open questions for what concerns the human rights implications of (some of the) current cybersecurity arrangements, especially in light of the government's obligation to uphold and protect human rights following from the Universal Declaration of Human Rights (1948).

This article connects the current debate on surveillance of communications with human rights. It departs from the assumption that mass surveillance 'amounts to a systemic interference with the right to respect for the privacy of communications' . It provocatively posits hackers and hacktivists as the guardians of human rights in cyberspace and of individual freedoms of expression, and the right to privacy in particular. It explores a side of the hackerdom which is unknown to (or deliberately ignored by) most cybersecurity policymakers – the politically motivated use of tech expertise to enhance transparency, raise awareness and shield users from industry snooping and state monitoring.

2. A question of vocabulary

A rich mythology has flourished around the figure of the hacker, often pictured as exceptionally talented individuals, perhaps socially awkward and ready to provoke or exploit chaos in the digital realm. Hackers have been called many names, from heroes to criminals, from cyber bandits to digital Robin Hoods, regardless of the enormous differences that exist within the worldwide hackerdom. In order to position the core argument of this article, we ought to start from what is in a world, as it can help us understand the connection between hacking, ethics, and human rights – and position the variety of tactics hackers and hacktivists use in the attempt to create a better cyberspace or safeguard online freedoms.

'Hackers are VERY serious about forbidden knowledge. They are possessed not merely by curiosity, but by a positive LUST TO KNOW,' wrote cyberpunk novelist Bruce Sterling back in 1993. He linked 'these young technophilic denizens of the Information Age' to 'some basic shift in social values' that emerge as 'society lays more and more value on the possession, assimilation and retailing of INFORMATION as a basic commodity of daily life'[5].

But the politicisation of hackers is somewhat of a recent phenomenon. The first 'computer hackers', who appeared in the 1970s around the Massachusetts Institute of Technology in Cambridge, MA, were intrinsically apolitical. Highly skilled software writers, they enjoyed experimenting with the components of a system with the aim of modifying and ameliorating it, and operated under a set of tacit values which soon became known as the 'hacker ethics.' Such ethical code included freedom of speech, access to information, world improvement and the non-interference with the functionality of a system ('leave no damage' and 'leave things as you found them(or better)'). Around the same time, software developers and user communities started advocating and practising freedom in managing and using computer technology, for instance targeting software to individual needs. They were the pioneers of what became known as the open source movement. Similarly to hackers, they promoted a hands-on attitude to computing and information more in general; but while hackers emphasised a 'do not harm' approach, open source advocates championed collective improvement and selfless collaboration.

Since the 1970s, hacking, as well as the open source movement, went a long way. Commonly, we distinguish between 'black hat' hackers who violate computer security with malicious intents like fraud or data theft, and 'white hat' hackers, who on the contrary perform hacking duties in view of repairing bugs or 'making things better.' Between the two, a plethora of nuances and variations can be found amongst the many people who self-identify as 'hackers,' including civic hackers who use data and software to ameliorate the state output but often have no particular programming skills and 'ethical hackers' who, for example, support security agencies in their fight against terrorism or report vulnerabilities with the scope of helping an organisation fixing them.

[1] Deibert, R. (2013). Black Code: Inside the Battle for Cyberspace. Toronto: Signal

[2] United Nations General Assembly, A/HRC/23/40, 17 April 2013; http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[3] Zittrain, J. L. (2008). The future of the internett–And how to stop it. New Haven and London: Yale University Press.

[4] Kravets, D. (2016). 'FBI vs. Apple is a security and privacy issue. What about civil rights?, ArsTechnica, 15 March; http://arstechnica.com/tech-policy/2016/03/fbi-v-apple-is-a-security-and-privacy-issue-what-about-civil-rights.

[5] Sterling, B. (1993). The Hacker Crackdown. Law and Disorder on the Electronic Frontier. New York: Batham, http://cyber.eserver.org/sterling/crackdwn.txt. Original capitals.

Hacktivism, in turn, represents a sort of activist evolution of early-day hacking. It involves the politically motivated use of technical expertise like coding: activists seek to fix society through software and online action. In other words, it is ‘activism gone electronic’[6]. The first recorded instance of hacktivism dates back to 1995, when a group of activists organised a netstrike, ‘a networked version of a peaceful sit-in’ targeting the French government in opposition to its nuclear experiments in a Polynesian atoll. In the mid-1990s, the US tactical media collective Critical Art Ensemble theorised electronic disturbance and electronic civil disobedience as new forms of political resistance exploiting one of the main features of contemporary societies, namely decentralisation[7]. Hit-and-run online direct action such as virtual sit-ins, ‘digital storms’ and denial of service attacks were presented as the virtual equivalent of blocking a company’s headquarters to send a message.

Fast-forward to the second half of the 2000s and hacktivism was popularised by online communities like Anonymous whose self-identified members engage in spectacular disruptive actions and nuisance campaigns using electronic civil disobedience in support of freedom of speech on the web (and more). The group and the moniker originated in online chat rooms dedicated to politically incorrect pranks, and although Anonymous later mutated into a politically engaged community, it maintained an orientation to the ‘lulz,’ a neologism that indicates the fun associated with pranks[8].

3. A matter of (hacker) ethicsn

To be sure, the ‘hacker’ rubric is highly contested today, as it is indiscriminately used to indicate a variety of phenomena. It subsumes different values, tactics and goals under its umbrella, from denial of service attacks to morally-motivated security breaches testing – not all of which are compatible. The hacktivists’ repertoire, for example, crashes with the freedom of information and no-damage philosophy of earlier generations of hackers, for whom closing down a website equals to censorship, no matter the content of owner of such website. Certainly, the most disruptive forms of hacktivism such as sabotage cross the boundaries of acceptable practice in liberal democracies. However, with the distinctions outlined in the previous session in mind, this article suggests to look at hackers and hacktivists as specific forms of democratic participation that are heavily mediated by and address digital technology and the Internet. In other words, they express and reclaim democratic agency. In a society doomed by increasing disaffection towards representative democracy and declining citizen participation, hacking and hacktivism represent a quest for participation and an exercise of direct democracy. As such, they have the potential of fostering personal and collective empowerment, participation and self-determination – while promoting literacy and transparency. Such forms should be tolerated, as they are manifestations of an emerging grassroots social force pushing the boundaries of liberal democracy and questioning the relationship between citizens and the state, and the role of the latter as the sole guardian of individual freedoms. Rather than enemies of democracy, hackers and hacktivists are the carriers of grassroots demands concerning the present and the future of our society.

Hackers and hacktivists engage in disruptive and pre-figurative action, trying to create here and now the cyberspace as they would like it to be. As such, they harbour a message for society, one that has human rights at its core, also when human rights are not explicitly evoked. Such message addresses issues of transparency, positive freedoms but also negative freedoms (e.g. a freedom from state monitoring and surveillance) and an idea of democratic participation in the first person. It is grounded on ethics of technology which are also ethics of society, by virtue of which the two are seen as intrinsically related and dependable. Disruptive actions like ‘watching the watchers’ enacted by Anonymous have the ability of raising awareness of the dangers of massive data collection and poor data storage, or dodgy data sharing practices; whistleblowing increases transparency; shielding users by means of, for example, encryption defends their right to privacy. As such, hackers and hacktivists embody and voice the ‘shift in social values’ Sterling detected back in the 1990s and can be rightly seen as ‘the new guardians of our civil liberties,’ as Coleman put it[9]. ■

[6] | Jordan, T. And P.A. Taylor(2004). Hacktivism and cyberwars: Rebels with a cause?. London: Routledge, p. 1.

[7] | Critical Art Ensemble (1996). Electronic Civil Disobedience. New York: Autonomedia.

[8] | Milan, S. (2015). Hacktivism as a radical media practice, in Routledge Companion to Alternative and Community Media, edited by C. Atton, pp. 550-560.

[9] | Coleman, G. (2013). ‘Geeks are the new guardians of our civil liberties,’ Technology Review, 4 February; https://www.technologyreview.com/s/510641/geeks-are-the-new-guardians-of-our-civil-liberties/.

ANALYSIS

2015 – A YEAR IN REVIEW, AS SEEN FROM THE SECURITY OPERATIONS CENTER

GAWEŁ MIKOŁAJCZYK
Gaweł is managing, building and growing the Cisco Active Threat Analytics (ATA) Security Operations Centre (SOC) in Krakow, Poland. He holds numerous industry certificates, including CCIE #24987, CISSP-ISSAP, CISM, CISA, C|EH and SFCE. Gawel is a frequent speaker at IT Security events, such as Cisco Live! Europe, PLNOG, EuroNOG, Security B-Sides, CONFidence, Cisco Connect, Cisco Expo and Cisco Forums.

1. Introduction

Adversaries and defenders are both developing more sophisticated technologies and tactics. For their part, bad actors are building strong back-end infrastructures with which to launch and support their campaigns. Cybercriminals are constantly refining their techniques for stealing money from victims and for detection evasion, as they continue to extract data and intellectual property. Let us review last year's threat landscape from the point of security operations, researchers and security practicioners. The data we are going to present is discussed in great detail, over almost 90 pages in the *Cisco Annual 2016 Security Report* co-authored by several organisations within Cisco, most notably already mentioned Active Threat Analytics, Talos Security Intelligence and Research, Security Research and Operations (SR&O), Intellishield Team, Cognitive Threat Analytics, Lancope and OpenDNS. For some part of this research, Cisco partnered with Level 3 Communications Threat Research Labs.

2. 2015 Threat Landscape

Angler – Exploit Kit of the Year

Cisco, with support from Level 3 Threat Research Labs and co-operation from the hosting provider Limestone Networks, identified and shut down the largest Angler operation in the United States. It is estimated to have been targeting 90,000 victims per day and generating tens of millions of dollars annually for the threat actors behind the campaign. One of the interesting features of the Angler operation was large number of unique referers and their low use frequency. We found more than 15,000 unique sites pushing victims to the Angler exploit kit, 99.8 percent of which were used less than 10 times. Most of the referers were active only for a short period and were immediately removed from operation after a small number of users were successfully compromised. In the July 2015 analysis, we noted that the peaks of the Angler in activity coincided with the various Hacking Team zero-day exploits (CVE-2015-5119, CVE-2015-5122).

Cisco determined that about 60 percent of the Angler payloads delivered through this particular operation were delivering some type of ransomware variant, the majority being Cryptowall 3.0. Other types of malicious payloads included Bedep, a commonly used malware downloader to install click-fraud campaign malware. Both Cryptowall and Bedep are designed to enable cybercriminals make a lot of money quickly, and with minimal effort.

SSHPsychos – DDoS Botnet of the Year

SSHPsychos, one of the largest distributed denial of service (DDoS) botnets ever observed by Cisco researchers, was significantly weakened by the combined efforts of Cisco and Level 3 Threat Research Labs.

The SSHPsychos DDoS network is a unique threat. It enlists tens of thousands of machines distributed across the Internet, it has the power to launch a distributed denial of service (DDoS) attack that cannot be addressed on an individual device basis. In this case, the botnet was being created using brute-force attacks involving secure shell (SSH) protocol traffic. At times, SSHPsychos accounted for more than 35 percent of all global Internet SSH traffic, according to analysis by Cisco and Level 3.

SSHPsychos, a brute-force login attack using several hundred thousand unique passwords is operational in China and the United States. After a successful login by guessing the root password, the brute-force attacks ceased. Twenty-four hours later, adversaries then logged in from a U.S. address and installed a DDoS rootkit on the compromised machines. This was a tactic to reduce suspicion from administrators. The botnet's targets varied, but in many cases appeared to be large Internet service providers (ISPs).

Cisco reached out to Level 3 Threat Research Labs. Level 3 analysed the traffic at IP netblock 103.41.124.0/23, confirmed that no legitimate traffic was originating or was destined for that address, and finally blackholed the network traffic for this netblock. It was a successful tactic, but soon, a new network netblock 43.255.190.0/23 emerged, showing large amounts of SSH brute-force attack traffic. Cisco and Level 3 decided to take action against 103.41.124.0/23, as well as the new 43.255.190.0/23 prefix.

Taking down the netblocks used by SSHPsychos did not permanently disable the DDoS network. However, it slowed down its creators' ability to run their operations and it temporarily prevented SSHPsychos from spreading to new machines.

Other Well Known Botnets

Well-known botnets like Bedep, Gamarue and Miuref represented the majority of botnet command-and-control (C2) activity. We found that during this period, Gamarue – a modular information stealer that has been around for years – was the most common command-and-control threat. The before-mentioned Angler exploit kit also delivers the Bedep Trojan, used click-fraud campaigns. In summary, those two and Miuref (a Trojan and browser hijacker that can perform click fraud) represented together more than 65 percent of the botnet C2 activity in the user base we analysed.

The percentage of Bedep infections remained relatively stable during the last year. However, a perceived decrease in Miuref infections was observed. We attribute this to the increase in HTTPS traffic. Encryption helped to conceal Miuref's indicators of compromise (IoC).

Malicious Browser Extensions

Malicious browser extensions are a major source of data leakage for businesses and are a widespread problem. We estimate that more than 85 percent of organisations studied are affected by malicious browser extensions. Our research indicates that browser infections are much more prevalent than many organisations may realise. From January to October 2015, we examined 26 families of malicious browser add-ons.

> “ Malicious browser extensions are a major source of data leakage for businesses and are a widespread problem.

Malicious browser extensions are delivered by software bundles or adware. They can steal information and be a major source of data leakage, by exfiltrating more the details about every webpage that the user visits. They are also gathering highly sensitive information embedded in the URL that can include user credentials, customer data and details about an organisation's internal infrastructure. They are also designed to pull in revenue by exploiting users, they can lead users to click on malvertising ads or pop-ups, and can distribute malware by tricking users to click a compromised link or to download an infected file.

Across the 45 companies in our sample, we determined that in every month we observed more than 85 percent of organisations being affected by malicious browser extensions – a finding that underscores the massive scale of these operations. We suggest that it is worth security teams' time to devote resources to monitoring this risk and to consider increased use of automation to help prioritise threats.

Domain Name System – Very Often a Blind Spot

Cisco's analysis found that the majority of that malware – 91.3 percent – uses the Domain Name Service (DNS) to carry out campaigns. To get this percentage, we mined all sample behaviors from a variety of sandboxes that we own. Malware that was determined not to use DNS in any way, was removed from the analysis. The remaining was using DNS to connect to sites that were validated as bad or were considered suspicious.

Why is DNS a security blind spot for so many organisations? 68 percent of security professionals report that their organisations do not monitor threats from recursive DNS, a reason being security teams and DNS administrators typically work in different IT groups within a company. And they do not talk to each other but they certainly should. Monitoring DNS is crucial for identifying and containing malware infections that are using DNS; it is also an important step in mapping out other components that can be used for further investigating an attack. Monitoring DNS takes more than collaboration between security and DNS teams, however. It requires the alignment of the right technology and expertise for correlation analysis.

Software Vulnerabilities Landscape

Adobe Flash vulnerabilities continue to be popular with cybercriminals. Overall Flash volume has decreased over the past year, yet it still remains a favored tool of exploit kit developers. However, there was no visible trend in Flash malware, neither increasing nor decreasing in 2015. It is likely to remain a pri¬mary exploitation vector for some time: the already-discussed Angler exploit kit authors heavily focus on Flash vulnerabilities.

> “ Adobe Flash vulnerabilities continue to be popular with cybercriminals.

Industry pressure to remove Adobe Flash from the browsing experience is leading to a decrease in the amount of Flash content on the web, a similar trend as with Java in recent years and which has, in turn, led to a steady downward trend in the volume of Java exploits. The Angler's authors don't bother to include Java exploits anymore. Meanwhile, the volume of PDF malware has remained fairly steady.

Microsoft Silverlight also has diminished as an attack vector. Many companies are moving away from Silverlight as they embrace HTML5-based technologies. Microsoft has clearly indicated that there is no new version of Silverlight on the horizon and is currently only issuing security-related updates.

Encrypted Traffic – Good For Privacy, Blinding The Defenders

The percentage of enrypted traffic in the total Internet traffic mix increases constantly. While not yet the majority of transactions, it will soon become the dominant form of traffic on the Internet. In fact, our research shows that it already consistently represents over 50 percent of bytes transferred due to the HTTPS overhead and larger content that is sent via HTTPS, such as transfers to file storage sites.

There is no excuse, however, to leave sensitive data unencrypted in transit. Security tools and their operators need to adapt to this new situation by gathering protocol headers and other non-encrypted parts of the data stream along with other sources of contextual information to analyse encrypted traffic. Tools that rely on payload visibility, such as full packet capture (FPC), are becoming less effective today. Running NetFlow and other metadata-based analyses is now essential. Also, High entropy is a good indication of encrypted or compressed file transfers or communication. Good news for security teams is that entropy is relatively easy to monitor, as it does not require knowledge of the underlying cryptographic protocols.

Let us examine some of the organisations that we are working with. At one of the universities we found that almost all internal traffic was encrypted (82 percent) and, in addition, 53 percent of the university's Internet traffic was encrypted. In healthcare environments the situation seems to be different – only 36 percent of one of the hospitals' internal data was encrypted. However, more than half (52 percent) of the Internet traffic was encrypted. Another example, inside a leading Internet Servie Provider network, 70 percent of the internal traffic and 50 percent of Internet traffic was encrypted.

Compromised Websites – Vehicle For Threat Actors

Threat actors are heavily making use of compromised Internet websites created using WordPress for their criminal activities. There they can marshal server resources and evade detection. While WordPress shows only 12 vulnerabilities for 2015 for its own product, a staggering additional 240 vulnerabilities come from third-party plugins and scripts. The number of WordPress domains used by criminals grew 221 percent between February and October 2015.

With WordPress sites, attackers can take control of a steady stream of compromised servers to create an infrastructure that supports ransomware, bank fraud or phishing attacks. We believe that this has happened for a reason – for example, communications that relay Cryptowall 3.0 ramsomware encryption keys through compromised WordPress servers may appear normal, thus increasing the chances that file encryption will be completed.

Security operators concerned about the threats posed by WordPress hosting by cybercriminals should seek content security technology that is able to perform deep web content inspection. Such traffic should be considered unusual at minimum if the users are downloading executables from WordPress sites instead of just webpages and images, although WordPress sites can host legitimate programs as well.

> “ Old network infrastructure devices leave organisations increasingly vulnerable to compromise.

Aging Infrastructure Problem

Many organisations built their network infrastructure a decade ago, when they simply did not account for the fact that the business would be 100 percent reliant on that infrastructure. Nor did they anticipate that their infrastructure would become a prime target for cyberattacks.

Old network infrastructure devices leave organisations increasingly vulnerable to compromise. We analysed 115,000 Cisco devices on the Internet and discovered that 92 percent of the devices were running software with known vulnerabilities. In addition, 31 percent of the Cisco devices in the field that were included in our analysis are "end of sale" (EoS) and 8 percent are "end of life" (EoL). Organisations tend to avoid making infrastructure updates because it's expensive and requires network downtime. What is more important, a simple update may not be enough, as many products are so old they cannot be upgraded to incorporate the latest security fixes needed to protect the business. Organisations need to plan proactively for regular upgrades and recognise the value of taking ownership of their critical infrastructure – before a cyberadversary does.

Time To Detection (TTD) is Decreasing

"Time to detection," or TTD, is defined as the window of time between the first observation of an unknown file and the detection of a threat. We determine this time window using opt-in security telemetry gathered from Cisco security products deployed around the globe.

From January to March, the median TTD was roughly the same – between 44 and 46 hours, but with a slight downward trend. However, by the end of May, TTD for Cisco had decreased to about 41 hours. Since May 2015, we have reduced the median time to detection (TTD) of known threats in our networks to about 17 hours – less than one day. This far outpaces the current industry estimate for TTD, which is 100 to 200 days.

How was it possible to decrease the TTD by half over the last year? First, the industrialisation of hacking and greater adoption of commodity malware played an important role in our ability to narrow the window on TTD. A threat that is industrialised becomes more widespread and thus easier to detect.

The decrease of TTD can be attributed not only to technology. We believe that combination of sophisticated threat defenses and close collaboration among security researchers has been even more critical to our ability to consistently and significantly reduce the median TTD over the course of 2015.

3. Summary. A Look Forward Into 2016

According to an October 2015 Cisco study of finance and line-of-business executives regarding cybersecurity's role in business and digital strategy, enterprise executives understand that protecting their businesses from threats may dictate whether they succeed or fail. As organisations become more digitised, growth will depend on their ability to protect the digital platform.

Business leaders are also anticipating that in 2016 investors and regulators will ask tougher questions about security processes, just as they ask questions about other business functions. Ninety-two percent of the respondents agreed that regulators and investors will expect companies to provide more information on cybersecurity risk exposure in the future.

> "Ninety-two percent of the respondents agreed that regulators and investors will expect companies to provide more information on cybersecurity risk exposure in the future.

Therefore, let's highlight six key points that should be an architectural cybersecurity discussion topics for year 2016:

1) A rich network and security architecture is needed to address the growing volume and sophistication of threat actors. An architecture which instead of just alerting security teams to suspicious events and policy violations, can help inform better decision-making around security. The traditional model for security has been "See a problem – acquire a new box." These solutions, often a collection of technologies, don't talk to each other in any meaningful way. They produce siloed information and intelligence about security events, which are integrated into an event platform and then analysed by security personnel.

2) Organisations invest in "best in class" security technologies, but how do they know if those solutions are really working? The headlines about major security breaches over the past year are evidence that many security technologies aren't working well. And when they fail, they fail badly.

3) More encrypted traffic will require an integrated threat defense that can converge on encrypted malicious activity that renders particular point products ineffective. As discussed in this article, encrypted web traffic is on the rise. There are good reasons for using encryption, of course, but encryption also makes it challenging for security teams to track threats.

4) Open APIs are crucial to an integrated threat defense architecture. Heterogeneous environments need a common platform that provides greater visibility, context and control. Building a front-end integration platform can support better automation and bring better awareness into the security products themselves.

5) An integrated threat defense architecture should require less gear and software to install and manage. This will help to reduce the complexity and fragmentation in the security environment that create too many opportunities for easy access and concealment for adversaries.

6) The automation and coordination aspects of an integrated threat defense will help to reduce time to detection, containment and remediation. False positives reduction helps security teams focus on what matters most. Contextualisation supports a front-line analysis of events underway, helps teams assess whether those events require immediate attention and can ultimately produce automated responses and deeper analytics. ■

ANALYSIS

RACE ON TALENTED PEOPLE – FINLAND CASE: WHAT KIND OF SKILLS ARE NEEDED?

DR ANTTI PELKONEN
Dr. Antti Pelkonen is as a Senior Scientist at Innovations, Economy and Policy research team at VTT Technical Research Centre of Finland. His area of specialisation is science, technology and innovation policy, policy evaluation and governance. He has over 15 years of experience in innovation policy studies and has participated in and headed numerous research and evaluation projects funded by European and national organisations. Recently he has headed a large-scale research project funded by the Prime Minister's Office which examined the current state and future perspectives on cybersecurity skills and expertise in Finland.

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

REIJO M. SAVOLA
Reijo M. Savola, is a Principal Scientist at the VTT Technical Research Centre of Finland. He received an MSc degree in Electrical Engineering from the University of Oulu, Finland in 1992, and a Licentiate degree in Computer Science from Tampere University of Technology in 1995. Mr Savola worked for Elektrobit Group Plc. in Oulu, Finland and in Redmond, Washington, USA for seven years before joining the VTT Technical Research Centre of Finland. His research interests include security metrics, modelling of security and bridging the gaps between various aspects of security engineering. He has published 165 journal, conference and workshop articles.

JARNO SALONEN
Jarno Salonen is a research scientist at VTT Technical Research Centre of Finland, who aims at making the digital world a better place for ordinary users. He has got a background of 15 years in the development of electronic services, role-based identity management, information security and privacy during which he has contributed in numerous national and international projects, as well as, applicable forums. His recent activities include defining cybersecurity competences in Finland, which was accomplished in a project coordinated by VTT as part of the analysis, assessment and research activities of the Finnish Government in 2015.

1. Introduction

Cybersecurity is a rapidly growing domain, not only in terms of business activities but also with respect to its significance for the societies as a whole. The demand for cyber expertise is huge as companies, public sector authorities, universities, research institutes and vast range of other organisations in the society need cybersecurity expertise and experts to protect their information and communication systems. This situation poses important challenges for cybersecurity competences and skills development. How can this demand for cybersecurity competences be met and what kinds of skills are particularly needed? What are the key elements in developing cybersecurity competences?

In this article we take a look at cybersecurity skills and competences both from global and national perspectives. We start from the global perspective and shed light on the global situation in terms of cybersecurity expertise. From the global scene we, then, switch to national perspective and study the cybersecurity skills and competence base in Finland, a country well-known for its ICT industry, and mobile technologies[1]. Finland has recently set very ambitious targets in terms of cybersecurity and it is, therefore, interesting to examine the current situation in terms of cybersecurity competences and skills in the country. Are there any preconditions in terms of skills and competences in Finland to become a world-leading nation in the cybersecurity area?

2. Global Perspective on Cybersecurity Skills

The human resources have always been the most valuable resource in cybersecurity and the value of talented individuals is increasing. Even if there is ongoing so called cyber arms race in the world, the most frantic contemporary race is about talented individuals. Of course, organisations, latest technologies and recourses are needed and they are important, but skilled and talented individuals are the most valuable part in cybersecurity. People are recruited from a global workforce, and states around the world compete for the limited number of experts. In addition, the private sector draws from the very same pool. At the same time, massive amounts of money are globally put into building cybersecurity solutions into the new innovations of robotics, big data, Internet of Things, and for example metamorphic networks. This development is a part of a large on-going trajectory: security and privacy of the digitalised world is becoming more strategic than ever before, and the skilled people of cybersecurity become very decisive factor in this development.

> “The human resources have always been the most valuable resource in cybersecurity and the value of talented individuals is increasing.

Examine the numbers and today's much publicised cybersecurity-skills gap starts to look worrying. Frost & Sullivan[2] predicts a shortfall of 1.5 million IT security professionals by 2020, while one in four organisations already faces a "problematic shortage" of cyber talents[3]. A report from Cisco puts the global figure at one million cybersecurity job openings in 2016[4]. Meanwhile, the fact that for example in the United Kingdom less than 0.6% of recent computer science graduates

[1] | The section on Finnish cybersecurity competences is based on recently finish research project called Cybersecurity competencies in Finland: Present state and roadmap for the future. The references to survey data, interviews and other data refer to data collected in this study. The data is described in the final report of the study. The report which includes an English summary is available at http://tietokayttoon.fi/julkaisu?pubid=9301.

[2] | Frost & Sullivan. 2015. The 2015 (ISC) Global Information Security Workforce Study. A Frost & Sullivan White Paper, London.

[3] | Gahm, Jennifer, and Bill Lundell. 2015. 2014 IT Spending Intentions Survey. ESG report. February 28.

[4] | Cisco. 2015. Mitigating the Cybersecurity Skills Shortage. 2015. http://www.cisco.com/c/dam/en/us/products/collateral/security/cyber-security-talent.pdf (access: 23.1.2016).

chose careers in cyber-security speaks for itself[5]. In the United States alone in 2014, companies posted 49,493 jobs that require Certified Information Systems Security Professional (CISSP) certification, a major cybersecurity qualification[6]. This lack of cyber specialists is more than just an inconvenience: it has dramatic implications for the security of nations, organisations and individuals. Competition is so fierce in the sector that security professionals on LinkedIn moved jobs more than twice as often as average workers in the year to April 2015[7]. On some occasions top cybersecurity experts are billing companies more than £10,000 a day to protect vulnerable IT systems from sophisticated hackers[8]. This can be seen as a part of today´s evolution since whenever rapid demand increase hits a profession with nontrivial skill and/or education requirements, economic theory suggests that rapidly rising compensation packages and strong competition for workers can be expected[9]. Access to talented people is rapidly becoming the critical factor in determining who stays ahead in the cybersecurity race against both criminals and state-sponsored actors.

Governments, intelligence services and private companies are looking for cybersecurity specialists, because their competences are needed more and more. For example in March 2014, US Secretary of Defense Chuck Hagel announced that the Pentagon is revamping its cyberforce[10]. USCYBERCOM will grow into a unit of 6,000 "cyberwarriors" by 2016, which under the current conditions is a tall order. In the US, also FBI is seeking to hire another 1000 agents to its cyber division by 2016, plus 1000 analysts[11]. The challenge for organisations is that they cannot get enough skilled cybersecurity people to join their service. Despite all different initiatives, the US Government has had to face also a serious problem of the migration of skilled specialists from government agencies to private industries. The talents are attracted especially by higher earnings and more attractive career paths in the private sector. This a global problem too. Other nations are facing exactly the problem. The demand for cybersecurity experts continues to rise, and it is not just the government and private companies in the United States that plans to boost its cyber capabilities.

Perhaps, the most important step in solving cybersecurity profession talent gap is making, especially the millennials, aware of the issue and the opportunities available to them in this growing field of carrier. Many simply do not know that the cybersecurity field of career is an option[12], and it results in little number of people entering the cybersecurity workforce. It also has to be remembered that even if the emphasis is put on hiring technologically talented individuals, the current very complex security environment where digital and physical worlds are in very close interaction with each other, probably the most valuable skills for cybersecurity career in next years may not be a focus in specific technology, but ability to understand the big picture as strategic thinkers.

[5] | Morgan, Lewis 2014, "Global Shortage of two million cybersecurity professionals by 2017", ItGovernance, October 30.

[6] | Cowan, Gerrard. 2015. "High-paying Cybersecurity Jobs Go Begging Across the World." Fortune. December 7. http://fortune.com/2015/12/07/high-paying-cybersecurity-jobs-go-begging-across-the-world/ (access: 24.1.2016).

[7] | Megaw, Nicholas. 2015, "Cybersecurity sector struggles to fill skills gap", Financial times, 18.11.2015.

[8] | ManpowerGroup. 2015. Christmas comes early for cybersecurity specialists. Report. December 8. http://www.manpowergroup.com/wps/wcm/connect/3f34d2d2-eb36-46e9-ae57-6a517f8aea65/UK_Release_1Q2016.pdf?MOD=AJPERES&CACHEID=3f34d2d2-eb36-46e9-ae57-6a517f8aea65 (access: 23.1.2016).

[9] | RAND Corporation. 2014. H4cker5 Wanted – An Examination of the Cybersecurity Labor Market. http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf (access: 28.1.2016).

[10] | Nakashima, Ellen. 2014. "U.S. cyberwarfare force to grow significantly, defense secretary says". Washington Post, March 28.

[11] | Simmins, Charles. 2014. "FBI looks to hire 1000 agents and analyst this year", ClearanceJobs, April 3.

[12] | Raytheon. 2015. Securing Our Future: Closing the Cybersecurity Talent Gap. Survey of Raytheon Intelligence, Information and Services. Sterling.

What we actually mean by saying skilled cybersecurity specialists? The term "cybersecurity" itself is very broad, and it is an area that does not have a single definition. Consequently, there are many different cybersecurity jobs, which requirements vary, and we should be more specific when we discuss the gap of cybersecurity talents. We also need to keep in mind that the skills that are needed today may be different in a few years time.

3. Cybersecurity Skills and Skill Gaps in Finland[13]

Recently, Finland has set itself ambitious targets in terms of cybersecurity. The national cybersecurity strategy, released in January 2013, stated that by 2016 Finland should become "a global forerunner in cyber threat preparedness and in managing the disturbances caused by these threats"[14]. Furthermore, new information security strategy, published in February 2016, puts forward a vision according to which "the world's most trusted digital business comes from Finland"[15]. As cybersecurity is a high-technology domain that requires high-level of expertise and specialised skills, it is relevant to ask what do such visions imply in terms of competences and skills development. What are the preconditions, especially in a small country like Finland, to become a world leader in highly competitive area like cybersecurity, and perhaps most importantly, what is the current competence base in the country and what might be the future competence needed?

Given the high-technology nature of cybersecurity, research, development and innovation activities are particularly significant in terms of competences (and competitiveness) in the domain. Hence, from the perspective of national skills and competence development the following strands of activities are important[16]:

1) Research at universities, research institutes and universities of technology. High level basic research provides the basis for competence development, higher education and new innovations. Similarly, applied research is important in terms of bridging the gap between basic research and commercialisation and innovation. Particularly important is thus the level and quality of various types of research activities in research fields relevant to cybersecurity such as: mathematics, information technology, information systems, programming etc.

2) Education at universities and universities of technology. Higher education is particularly important in terms of development and continuity of competences as well as the amount of experts and the national competence pool. In practice, this refers in particular to the scope and quality of tertiary education and curricula in cybersecurity relevant subjects.

3) Business activities and entrepreneurship. The quantity, scope and quality of companies operating in the cybersecurity domain, as well as, their orientation with respect to product development, R&D activities, growth and exports are significant. In addition, particularly important is collaboration and interaction between companies, universities, research institutes and public sector authorities, hence

[13] | This section draws heavily on the following report: Pelkonen, Antti, Toni Ahlqvist, Anna Leinonen, Mika Nieminen, Jarno Salonen, Reijo Savola, Pekka Savolainen, Arho Suominen, Hannes Toivanen, Jukka Kyheröinen & Juha Remes (2016). Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. http://tietokayttoon.fi/julkaisu?pubid=9301 References to data refer to data collected in this study.

[14] | Council of State. 2013. Finland's Cybersecurity Strategy. Government Resolution. 24.1.2013. http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

[15] | Ministry of Transport and Communications. 2016. Maailman luotetuinta digitaalista liiketoimintaa. A working group's proposal for Finland's information security strategy. http://www.lvm.fi/documents/20181/877203/Julkaisuja+4-2016/795a8541-7ef5-4690-967d-a1861f1a8a48.

[16] | In addition to these three competence factors, a number of framework conditions and other aspects such as legislation, public R&D funding, lifelong learning schemes and general awareness of cybersecurity issues, are significant for cybersecurity competence development.

the degree to which these actors are able to form a well-functioning cybersecurity 'ecosystem'.

In the following, we will shortly discuss each of these three key aspects of cybersecurity competence development from the perspective of Finland. After that, we will address the competence gaps identified in the Finnish cybersecurity domain.

4. Competence Development: Cybersecurity R&D and Education in Finland

In terms of research, Finland has historically relatively strong competence base in engineering sciences, and as a part of that also in information technology. Research activities in information technology were started in Finland in the 1950s, and the first professorships in information technology were established in the 1960s[17]. In the 1970s and early 1980s, development in microelectronics was very fast, and research and development in these areas were broadly further developed in Finland. In the following decade, higher education in ICT-related fields was strongly increased which was related to the demand created by the fast rise of Nokia's mobile phone business[18]. Overall, Finnish research in computer and information science has been regarded high level, but recently, it also has been estimated that the quality of research has declined and the risk is that it may not be at the level of world leading countries any more.[19] Similarly, Finnish research in mathematics has been considered of the particularly high quality in international and national evaluations, especially with respect to the small population of the country and particularly in certain specific areas such as discrete mathematics and inverse research[20]. However, the same evaluations have stated that mathematical fields related to information technology such as: algebra, cryptography and mathematics of signal processing have been relatively weakly developed in Finland. Research activities that are specifically related to cybersecurity have significantly increased in Finland since the mid-1990s. In terms of scientific publications, for instance, the volume of research has quadrupled between mid-1990s and 2013 (Figure 1). Despite the growth, the volume of research is still relatively small: there are only a bit over 10 university professors focusing on cybersecurity issues and the annual number of scientific publications is around 130. Furthermore, research activities are scattered around 16 universities, research institutes and universities of technology. which implies that research units are small on average. Despite the relative small overall volume, there are world-class research and narrow spearhead research areas, such as: cryptology, vulnerability research, mobile security and information security management. These are, however, often on a very narrow basis and based on the work of one or few leading researchers.

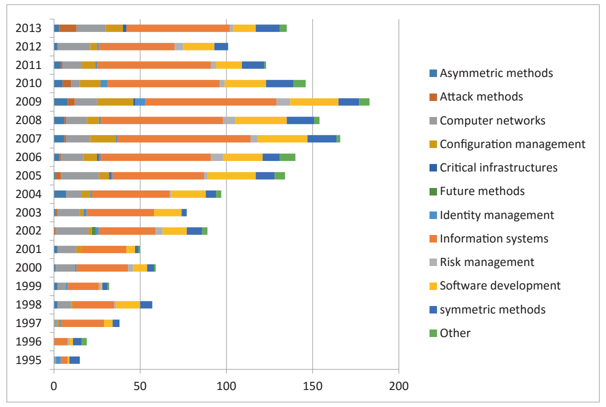


Figure 1: Scientific publications in cybersecurity in Finland 1995-2013. Source: Web of Science[21].

[17] | Pelkonen, Antti. 2003. Tieto- ja viestintäteknologia teknologiavetoisen yhteiskunnan rakentajana ja yhteiskuntapolitiikan välineenä. Politiikka 45:1, 50-61.

[18] | Ali-Yrkkö, Jyrki & Hermans, Raine. 2002. Nokia Suomen innovaatiojärjestelmässä. Yliopistopaino, Helsinki.

[19] | Academy of Finland. 2012. Computer and Information Science. Background report to State of Scientific Research in Finland 2012 Report. http://www.aka.fi/fi/tiedepoliittinen-toiminta/tieteen-tila/aiemmat-arvioinnit/tieteen-tila-2012/

[20] | Academy of Finland. 2000. Evaluation of Finnish Mathematics. Report of the evaluation panel. 5/2000. Unpublished.; Academy of Finland. 2012. Mathematics and Statistics. Background report to State of Scientific Research in Finland 2012 Report. http://www.aka.fi/fi/tiedepoliittinen-toiminta/tieteen-tila/aiemmat-arvioinnit/tieteen-tila-2012/.

[21] | We are grateful to Arho Suominen for the analysis concerning Finnish scientific publications in cybersecurity.

With respect to education and training, higher education activities related to cybersecurity have broadened in Finland during the last years. Currently, there are 14 universities and universities of technology. that provide education in cybersecurity related themes[22]. In most universities, education in cybersecurity is organised as minor subjects or dedicated courses in subjects such as: information technology, telecommunications and information systems. In two universities, there are specific master's programmes in cybersecurity. These two programmes are both recently established and have, to some extent, systematised education in the area. They are, however, relatively small in terms of student numbers as both programmes take 20 new students annually. In a comparison to Estonia, which has less than quarter of the population of Finland, the Tallinn University of Technology alone takes 30 new students annually in the International Master's programme specialised in cybersecurity and digital forensics.

Similarly to research, cybersecurity business started to develop in Finland in the 1990s and the development took off especially around three companies: Data Fellows (currently F-Secure, established in 1988) which focuses on anti-virus products, Stonesoft (currently part of Intel, established in 1990) which concentrates on firewalls, and SSH Communications (established in 1995) which focuses on cryptography products. In the area of consulting and services, Nixu, established in 1988, has been a frontrunner in Finland. In addition, Nokia has also played a role in the emergence of Finnish cybersecurity cluster as it had a relatively small but significant information security research group until early 2010s. Nokia has also been an important customer for a number of cybersecurity companies.

Overall, Finland has currently relatively strong and broad business sector in cybersecurity area: there are approximately 80-90 companies which core business deals with cybersecurity. In addition to that, there is a large number of other ICT and telecommunications companies which have business and expertise in cybersecurity while their core business is in other areas. In relation to population, Finland has relatively large cybersecurity business sector in international terms. Yet, there are still countries with larger cybersecurity company base per capita, like Israel for instance.

In the business sector, there are strong areas of competence such as anti-virus expertise, identity and access management, firewalls, testing, and information and cybersecurity services for instance. The sector is also growing strongly: over the period of last three years, turnover of the companies in the sector has grown by 26 per cent on average. In 2014, Finnish cybersecurity companies employed approximately 4500 people and had a turnover of over 1 billion euros. Large part of the Finnish companies are, however, relatively small in size which is a challenge for instance in terms of internationalisation and export activities.

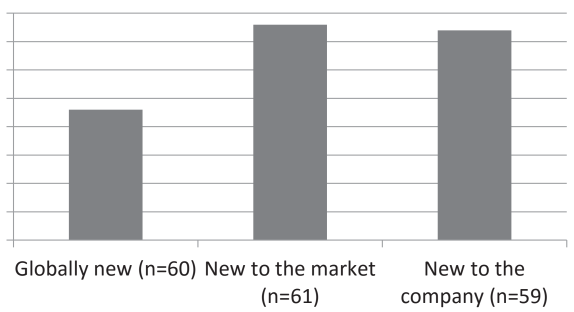


Figure 2: Number of companies who have introduced. innovations that are globally new, new to the market or new to the company during the last 5 years. Source: Survey to Finnish cybersecurity companies, autumn 2015.

Finnish cybersecurity companies clearly have also a potential and an ability to innovate: in our survey nearly 40 per cent of the companies (23/60) responded that they had introduced globally new innovations during the last 5 years (Figure 2). This

[22] | Lehto, Martti & Kähkönen Aili. 2015. Kyberturvallisuuden kansallinen osaaminen www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf.

is quite a large share as globally new innovation implies that similar product or services has not been available in any market world-wide. In addition, over half of the companies had introduced new to market or new to the company innovations.

5. Cybersecurity Competence Gaps

Despite the increased higher education and research activities, the shortage of cybersecurity specialists is also visible in Finland. This is particularly evident among cybersecurity companies: nearly 60 per cent of the companies (35/61) that responded to our survey were of the opinion that skilled labor force is not well available in the country. In practice, this has manifested in recruitment problems as companies have had challenges in recruiting experts for instance in areas like: cryptography, programming and identity and access management. Similarly, many of the public sector authorities responsible for cybersecurity issues have also experienced challenges in recruiting experts. In public sector, the challenge is more complicated because the public sector organisations are not able to compete with the private sector in terms of salaries. Competence gaps in the public sector recruitments have been visible in areas such as: cryptography, strategic and broad-based cybersecurity competences (experts with technical expertise and strategic understanding of cybersecurity) and, for instance, expertise related to investigating information security breaches.

It is also evident that higher education in the cybersecurity area is currently not sufficient in Finland. In our surveys, majority of company respondents (70 per cent) and university and research institute respondents (60 per cent) were of the opinion that the volume of high-level education is not at the adequate level. More education and more diversified training are thus needed. However, it is evident that cybersecurity is the area where one cannot learn all the necessary skills at the university or universities of technology, but in practice many of skills and competences are learned in hands-on projects in the workplace. Hence, often the expertise is further developed at work, but basic understanding and skills have to be gained through studies.

In addition to the above-mentioned areas of recruitment challenges, we have identified three broad areas where there are particular gaps or shortages of expertise in Finland. First area of competence gap is cryptography and, in particular, theoretical cryptology. As a matter of fact, cryptology is, somewhat paradoxically, currently both strength and weakness in Finland: there is very high-level expertise in the area but it is on a very narrow basis. Second area where there are few competences in Finland is non-technological, multidisciplinary expertise related to cybersecurity. While technical expertise is broadly at a high level in Finland, broad-based and multidisciplinary perspective in cybersecurity issues is more vaguely developed. This includes, for instance, areas such as: human and user aspects, behavioral perspective, as well as economic, legal and strategic aspects related to cybersecurity. These are particularly important dimensions, as along with the deepening of digitalisation it apparently becomes increasingly important to gain a more profound understanding of the cyberspace and its security.

Also the third area of competence gap in Finland deals with a non-technological domain: marketing, commercialisation, sales and export skills related to cybersecurity. This actually concerns a "traditional" and well-known competence shortage in Finland as Finns are known to be good engineers and product developers but not as good in marketing, selling and branding the products. This situation is clearly visible also in the cybersecurity area. For instance, many experts interviewed for our project maintained that Finnish solutions and products often are at least as good as products that have been successful in the world market, and that the difference is made in the ability to sell and market the products. In addition to these three broad areas, other, more specified areas, with fewer competences can be identified such as digital forensics and cyberattacks. Future competence needs are extremely difficult to anticipate due to the fast technological development in the cybersecurity area.

> "Skills that are needed are unquestionably vast and diverse and they will comprise technological but also increasingly non-technological competences.

Skills that are needed are unquestionably vast and diverse and they will comprise technological but also increasingly non-technological competences. The breakthrough of Internet of Things, emergence of cloud services, the development of 5G technologies, and the increasing use of big data will undoubtedly be significant for cybersecurity competence needs. Given the expanding nature of cybersecurity domain and its increasing significance, competences that are related to broad-based, comprehensive and strategic perspective on cybersecurity issues will probably be more important. Similarly, the understanding of cybersecurity aspects in the top management of organisations and higher hierarchies of political decision-making will gain more significance.

6. Conclusions

On the basis of our review of recent developments both internationally and in Finland, it is clear that the demand for cybersecurity experts and expertise has recently substantially increased, and it will further grow in the near future. This raises the questions of how to tackle the growing need for cybersecurity expertise and how national governments, educational systems and training schemes around the world should respond to the situation. Another important issue concerns the broader picture related to educational situation: Do we actually know, for instance, how cybersecurity related education has been developed recently in Europe? Has relevant education been increased and if it has, to what extent?

Regarding cybersecurity competences, the actual content and substance of the expertise and competence gap areas are of a particular importance. What are the substance areas where expertise is particularly sought after? On the basis of our study of cybersecurity competences in Finland, we highlight the following three areas and aspects that, according to our knowledge, may also have broader resonance in Europe and beyond.

First, an important area of cybersecurity competence which currently tends to have weight concerns multidisciplinary and strategic expertise. Cybersecurity is easily regarded as technical subject matter, which is, of course, natural regarding the main characteristics of the field. However, along with digitalisation the societal significance of cybersecurity will probably further increase and cybersecurity will be increasingly penetrating the society. This will increasingly require that technical cybersecurity competences are complemented with expertise from other disciplines and domains. Hence, the demand for experts with technical cybersecurity competences but also related broader, strategic, managerial, legal, and social scientific competences will probably grow.

> "Understanding of cybersecurity aspects in the top management of organisations and higher hierarchies of political decision-making will gain more significance.

Another key competence area concerns marketing and commercialisation skills related to cybersecurity technologies. Our study revealed that in Finland a large part of the cybersecurity companies are small and they experience particular difficulties in expanding their operations to new geographical markets. At the same time the domestic market is small and it is vital for the companies to be able to export products and services. Although there are some big players, in the European scale many promising companies in the sector are relatively small, and domestic markets in European countries are often limited in size. Hence, the ability to sell, market and, especially, export is increasingly significant for many companies in the sector.

Last but not least, in the cybersecurity area the threat landscape and technologies evolve continuously and technological change is fast. This means that also the needed skills and expertise profiles change over time, and as a matter of fact, they may actually change rapidly. In this situation it is relevant to ask how it is possible to guarantee that suitable expertise is available. One answer would be that there should be regular foresight exercises to examine the evolution of the field, the related future competence needs and the change that is taking place in terms of skill demand. Given the fast pace of technological progress, another answer would be that it is important to make sure that competences in the basic "domains" of cybersecurity, such as: mathematics, programming, and computer science, are kept at a high level. If the foundations are on the solid ground, it is easier to move to new areas and applications according to the upcoming demand. ■

POLICY REVIEW

2016 – CRITICAL YEAR FOR EU CYBERSECURITY?

JAN NEUTZE

Jan Neutze is Director of Cybersecurity Policy at Microsoft responsible for Europe, Middle East, and Africa (EMEA). In this role Jan works with policy and technical stakeholders on a range of cybersecurity issues, including security strategy and policy, cloud security, risk management, and critical infrastructure protection. In 2015, Jan was appointed by to the Permanent Stakeholders' Group (PSG) of the European Network and Information Security Agency (ENISA) to advise the organization's leadership on cybersecurity. Before taking on Microsoft's EMEA security portfolio, Jan worked in Microsoft's Trustworthy Computing (TwC) group at Microsoft Corp. in Redmond, WA. Jan came to Microsoft from the United Nations Headquarters where he led a range of projects focused on cybersecurity and countering terrorist use of the internet.

1. Introduction

After three years of intense negotiations, the EU finally reached agreement on the Network and Information Security (NIS) Directive this past December. The text has been finalised and will be formally adopted by the European Parliament and the Council of the EU in the coming months. Then, Member States will have 21 months to implement this landmark legislation. At a technical level, however, there is still work to be done. But more on that later.

> “ The Directive, as adopted, is also more likely to increase cybersecurity readiness across the EU.

While the adoption of the Directive is laudable, the process of finalising this Directive took over three years from when it was first proposed in February 2013. What at times must have seemed like an arduous and thankless process will now set the EU cybersecurity baseline for years to come.

The Directive, as adopted, is also more likely to increase cybersecurity readiness across the EU, given its tighter focus on outcomes and the effectiveness of the obligations introduced. It is also positive to see that all Member States are adopting a national cybersecurity strategy and establishing new national authorities dedicated to cybersecurity, as well as Computer Security Incident Response Teams (CSIRTs). The commitment to greater international and intra-European coordination is equally encouraging. In a positive result, the Directive generally pursues a risk-based approach to cybersecurity and rightly concentrates government resources on protecting critical infrastructure ("operators of essential services"), making an important distinction between those providers and "digital service providers" (DSPs) those who support aforementioned essential services, by assigning them different sets of obligations. The question of "What's next?" with regard to cybersecurity in the EU in general – and the implementation of the NIS Directive specifically, however, is not free from challenges. Three core issues regarding NIS implementation should be addressed:

A. Regulatory Harmonisation across the EU28: Critical Infrastructures

As mentioned above, the compromise found between the Council and the European Parliament entails different approaches for national critical infrastructure providers (referred to as "providers of essential services" in the Directive) and "digital service providers."

The approach pursued for critical infrastructures enables Member States to retain a significant degree of control over both entities which will be designated an "essential service" at the national level and it provides flexibility with regard to implementation of NIS requirements such as baseline security measures (referred to as *"appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems which they use in their operations"* in Art. 14(1), NIS Directive) and incident reporting (Art. 14(2), NIS Directive). While the Directive provides some guidance for how Member States should identify operators, i.e. in Recital 23 which reads *"…Member States should adopt national measures which will determine which entities are subject to NIS obligations. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria (e.g. output of the operator or number of users) which would allow to determine which entities are subject to NIS obligations and which are not."*

The reality of this approach is that the determination of which services are deemed to be critical infrastructures in Europe will continue to vary greatly across the EU28 respectively. As the criticality of a particular service is considered a national security issue by numerous Member States, agreement to further harmonisation in this context was politically not feasible during the NIS negotiations.

As for the adoption of security baseline measures for the respective critical infrastructures sectors (see Annex II of the NIS Directive), very little guidance exists in the Directive as to harmonising these measures. Many Member States pointed out during the negotiations that the approach chosen by the European Commission in proposing a Directive and not a regulation was one of "minimum harmonisation" – nowhere is that more apparent than in this context. The establishment of a (more technical) CSIRT network and a (more political) "co-operation group" linking up national competent authorities across all Member States – while helpful – will likely not prevent the fragmentation that is expected to result from this.

Three scenarios, therefore, seem possible: Member States will favour their existing national cybersecurity risk management schemes, develop new ones (which in a worst case scenario could conflict with existing international standards), or borrow from existing international approaches (such as the NIST Cybersecurity Framework developed in recent years in the United States). Incident reporting frameworks will likely also differ at the Member State level, though the Directive does offer some guidance in this context: Art. 14(6) of the Directive states that *"Competent authorities acting together within the cooperation group may develop and adopt guidelines concerning the circumstances in which operators of essential services are required to notify incidents…"*

The extent to which EU Member States are able to harmonise the requirements will set the standard for judging the success of the Directive in years to come. Looking at the EU's approach to network and information security among its national critical infrastructures, however, leads to the conclusion that continued fragmentation seems inevitable. While the NIS Directive provides some attempt at a coherent framework, Member States will likely continue to pursue separate, national approaches to one of Europe's most critical security issues. This may not seem like a problem for many operators providing services in only one Member State.

> “ The extent to which EU Member States are able to harmonise the requirements will set the standard for judging the success of the Directive in years to come.

The reality today, however, is that even among critical infrastructures many providers operate in more than one EU Member State (take banking or transport) – as do those who supply services to these entities, all of whom will be affected by disparate (and potentially conflicting) sets of NIS requirements. Moreover, lack of common baselines for critical infrastructures (not an insignificant segment of the European economy) will hinder and not help secondary markets (such as insurance) from developing.

B. Regulatory Harmonisation across the EU28: Digital Service Providers

The situation is slightly better in the context of so-called "Digital Service Providers." The European Parliament initially had excluded DSPs from the scope of the Directive and focused on addressing significantly greater risks of serious cyberincidents emanating from critical infrastructures. In light of sufficient opposition to this approach among some Member States, the Council and the Parliament ultimately agreed to include a subset of DSPs in the Directive's scope, specifically 1) online marketplace, 2) online search engine, and 3) cloud computing service.

One of the core concerns shared by nearly all stakeholders was that regulatory fragmentation for digital services – nearly all of which are available in each of the Member States – would create an undesirable regulatory burden, not just for established players but also for small and medium enterprises trying to be successful in Europe's Digital Single Market. The approach chosen regarding NIS implementation for DSPs thus consists of three core elements:

1) The European Commission has been tasked to develop secondary legislation in the form of two implementing acts which will harmonise both the security baseline and incident reporting requirements for DSPs – according Art. 15a(4)(4a)(4b).

2) Moreover, "When adopting implementing acts related to the security and notification requirements for digital service providers, the Commission should take utmost account of the opinion of ENISA and should consult interested stakeholders" according to Recital 72 of the Directive.

3) And finally, the issues of jurisdiction and applicable law for DSPs have been clarified to avoid potential overlap. Art. 15c/d specifies that: "For the purposes of this Directive, a digital service provider shall be deemed to be under the jurisdiction of the Member State where it has its main establishment. A digital service provider shall be deemed to have its main establishment in a Member State when it has its head office in the Union in that Member State."

This means that DSPs will face a harmonised set of requirements which Member States will need to implement accordingly. DSPs will, in principle, also have clarity regarding the jurisdiction within which they will be regulated. While it is particularly important that the transnational nature of the online environment has been recognised and that governments are committed to greater harmonisation of requirements for digital services, some important details need to be worked out.

The European Network and Information Security Agency (ENISA) is tasked to develop guidelines for security and notification requirements with input from other relevant stakeholders – but it remains to be seen to what degree the European Commission will model its implementing acts upon that guidance. ENISA's ability to coordinate with both governments and the private sector will be critical in order for this process to yield effective and workable results in a relatively short timeframe. This is particularly true with regards to developing an effective cybersecurity incident reporting scheme – the first of its kind for the technology sector.

Moreover, the Commission will need to pay close attention to Member States actually implementing legislation that reflects the framework for DSPs provided through the implementing acts. Many Member States did not want to wait for the NIS to be adopted and have already proceeded with national cybersecurity legislation – in several cases this will likely need to be adjusted once these implementing acts have been adopted.

> "Strong and effective collaboration between Member States and DSPs both at the technical and political level will be critical.

And finally, it remains to be seen how a Member State with jurisdiction over a digital service provider is able to engage with other Member States which do not – in particular in case of a serious incident affecting them also. Strong and effective collaboration between Member States and DSPs both at the technical and political level will be critical.

2. Conclusion

The potential for this law to be viewed as an international model hinges on the ability of Member States not only to develop new, complementary requirements, but also to align existing ones. Countries such as Germany, France and the Czech Republic have already adopted their own implementation of the NIS Directive ahead of its adoption.

However, this will not be the only area the EU will focus on. In late 2015, the European Commission launched a new consultation on how to establish a contractual public private partnership (cPPP) on cybersecurity, which is part of the EU's Digital Single Market Strategy. The PPP is expected to become operational by mid-2016, which is an ambitious timeline. The consultation also includes issues vital to increasing the level of network and information security across Europe: certification, standardisation and labelling. In responding to the cPPP consultation, many stakeholders voiced their concerns about the approach chosen by the European Commission, in particular regarding what some have called a "fortress Europe" approach. Digital Europe, a trade association representing 37 national trade associations from across Europe, stated in their response: *"We wish to stress that when it comes to cybersecurity, what is most important is the protection provided by a solution, rather than the specific geographical origins of a solution. We urge caution against the implementation of policies within the field of cybersecurity that focus on any goal other than the effective protection against threats. These threats are today global in nature and will remain so regardless of their target or origin. We are concerned about some questions within this consultation which ask organisations about their reasons for choosing "non-European ICT security products/services over European ones". We wish to stress that the origin of a security product or service should not play a role in judging its effectiveness or performance. We fully support the strengthening of the EU's ability to produce competitive cybersecurity products and services. The EU should continue to work to attract investment and resources to develop and strengthen this sector of the economy. However, this should not be done by displacing (or substituting) non-European solutions from the Single Market. Doing so risks lowering Europe's protection from cybersecurity threats as the highest quality products, regardless of their origin, should be available on the marketplace to provide for effective protection. Defending European cyberspace requires a global mindset, not isolation. Isolation risks higher threat exposure, weaker defences, and the inability for European players to scale up at the rate necessary to become competitive."*

The adoption of the NIS Directive, its effective implementation across the Member States – including by strengthening the role of ENISA – and the launch of the cPPP could make 2016 the year that shifts cybersecurity in Europe from a topic of conceptual debate to becoming the concrete foundation that is so urgently needed, and which will become the cybersecurity baseline framework for decades to come. It is time to roll-up our sleeves – and to get it right. ■

POLICY REVIEW

INCIDENT REPORTING IN THE CONTEXT OF CRITICAL INFRASTRUCTURE

PIOTR CIEPIELA
Senior Manager in Operational Technology Advisory, EY. He is a co-author and leader of consulting services in the field of Critical Infrastructure security and industrial automation systems for Central Europe (23 countries). He managed numerous projects in the United States, Europe and the Middle East. He participates in the creation of international standards for Cybersecurity and Industrial System Security (ISA and NIST), and acts as independent CIP Expert in the CIRAS Methodology development funded by EU. He lectured at major Polish universities and has authored numerous publications on ICS Security e.g. published in Harvard Business Review. He holds a security clearances: „NATO SECRET," „EU SECRET."

LESZEK MRÓZ
Senior OT Security Consultant in Operation Technology Advisory, EY. He has conducted numerous security assessments and participated in security programmes for Critical Infrastructure operators from oil & gas, power & utilities sectors. He has gained international experience during various projects performed in multinational teams for government institutions as well as for some of the largest enterprises in Europe, Middle East and North America. Actively contributes in the development of best practices guidelines for Critical Infrastructure operators in Europe.

DR TOMASZ WILCZYŃSKI
Manager in the EY's Advanced Security Center in Poland – competency centre for technical IT security services, part of the Cyber Security department. He managed or participated in numerous projects in the area of cybersecurity. Graduated from University of Science and Technology in Kraków and obtained Master of Science Degree in Telecommunications, as well as Bachelor of Arts Degree in the area of cybersecurity services in Financial Management from Oxford Brooks University. He also finished PhD studies in the area of Economics at Warsaw School of Economics.

1. Introduction

In 2004, the European Council decided to establish a foundation for European Programme for Critical Infrastructure Protection (EPCIP) in order to develop a strategy for protection of systems which are crucial to the functioning of societies in the EU Member States. Since then, the significance of the Programme in the context of cybersecurity is continuously rising, both for the European MS governments which are actively seeking efficient methods of protection against a new kind of threat – cyberwar, and Critical Infrastructure (CI) Operators who are facing new kind of risks in continuity of their critical business processes. One of the key factors which increase the importance of the Programme is the line of evolution of industrial automation and control systems (IACS) responsible for monitoring and direct control of numerous critical processes of every country, such as: production, transmission and distribution of energy, fuel extraction, processing and storage, distribution of drinking water and many more. In the last two decades, these systems have transformed from isolated nodes to integrated elements of IT/OT environment, where OT stands for Operational Technologies – hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise (Gartner) which, therefore, become opening to the cybersecurity risks and possibility of being disrupted or even taken over by attackers from outside of organisation.

One of the EPCIP work streams includes development of measures to reduce vulnerabilities, as well as performance metrics. To achieve success in this area, defining methods of information gathering and – what is more – information sharing is crucial. This include sharing knowledge and experience on good practices for the CI protection and on the security incidents which occurred within CI boundaries. In the world of continuous race between hackers and people responsible for security sharing information on actual incidents and analysis of their roots is an important factor for a numerous reasons. One is the possibility of protection of other operators from similar threats by controlled propagation of knowledge about vulnerabilities and methods for their mitigation. The others include, but are not limited to: necessity of understanding of trends in attackers' behaviour to develop security measures for newly emerging threats – in advance, or to define the most adequate programmes on the government and security association's side.

The importance of digital trust and cybersecurity is resulted in a proposed by Commission in 2013 "The Network and Information Security (NIS)" Directive which is currently in the stage of finalisation. Directive, among others, aims at strengthening Member States' national cybersecurity capabilities and improving co-operation between Member States (both between public and private sectors). In addition, it will introduce the obligation of incident reporting of the "essential services" operators to the national authorities.

This article is the first of a series which will discuss challenges related to incidents reporting and response rising from the operators' perspective with particular emphasis on OT solutions. However, it is worth highlighting that these challenges are not only applicable to OT environments. Appropriate handling of cyber incidents and effective communication to manage the outcome is also a key topic for organisations utilising only Information Technology (IT) systems as well. In many cases IT systems are also considered as a critical infrastructure due to the criticality of the stored or processed data.

2. Description of incident management process

The ITIL defines incident as an event which is not a part of the standard operation of the service and which causes, or may cause, an interruption or a reduction of the quality of the service. There are other numerous standards which describe good practice of incident management from the security perspective. Besides ITIL, the most recognisable and available publications include: National Institute of Standards and Technology (NIST) Special Publication 800-61 R2 or North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection CIP-008. Also, the new version of industry oriented IEC 62443-2-1 standard which is currently in the final draft will most probably include sections dedicated to the information security incident management.

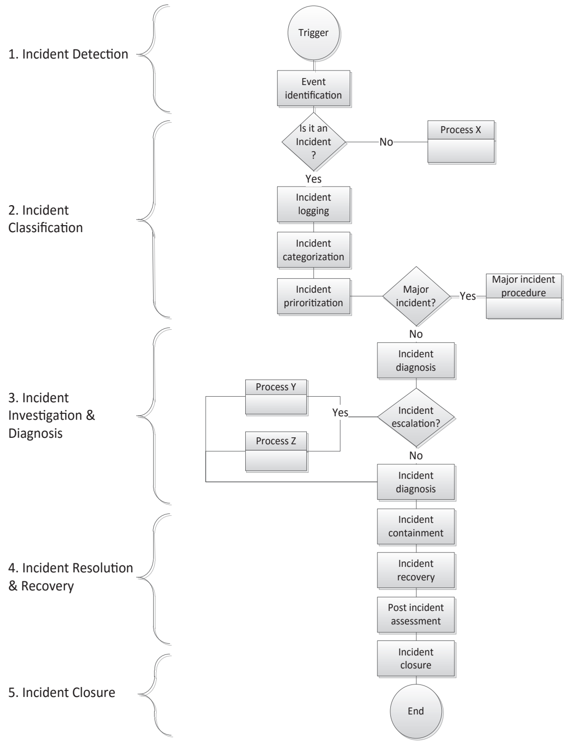


Figure 1: Incident management process.

Figure 1 presents general steps of incident management process. They can be divided into five general stages[1]:

A) **Incident Detection** – one of the most challenging elements of the process. It is not uncommon for organisations to believe they are safe and without any incident occurrence, when in fact they were just not able to detect it. Incident may be detected with the use of numerous automated security solutions, such as: antivirus, Intrusion Prevention/Detection Systems (IPS/IDS) or SIEM solutions. But even with advanced security systems in place it is still possible for incident to occur without detection or just the opposite – organisation gets lost in a flood of alerts generated from events which, in the end, do not classify as incidents (false positives). Detection process is even more challenging in OT environment, full of specific, intelligent (programmable) assets which can be subject to the attack but for which there is a shortage of available monitoring solutions. Although general trend is that companies are implementing a dedicated OT monitoring systems, the overall number of implementations is still small in comparison to the number of organisations that are a potential target of an OT-aimed attack. Also, implemented solutions are in most cases compatible with only the most common OT assets (vendors), without out-of-the-shelf libraries for more rare PLCs, programmable inverters, intelligent sensors or actuators. As the characteristic feature of the OT environment is a much greater share of obsolete systems than in a standard IT, the OT assets are very often protected mostly by services on the boundaries of corresponding network. This makes it much more difficult to protect against attacks conducted by people within organisation (intentional or unintentional) who have physical access to an element of industrial control systems.

B) **Incident Classification** *(When it covers also verification and incident assignment, this stage may be called "Triage")* – when incident is detected, it has to be evaluated to form a decision on the path of its resolution and recovery. Each organisation may introduce its own classification model, depending on the structure of its assets, but in general the first step is to assess the incident and the business impact it has/may have and urgency of resolution, then to assign it to the incident category determining the most feasible resources (e.g. personnel location and competences). From the OT perspective the main difference in incident prioritisation is that very often permissible unavailability of the service is 0, moreover, the availability and integrity of information have influence on the condition of physical infrastructure. Therefore, even a relatively small disruption in system operations may have a significant impact, not only economical but also on human life and health or natural environment.

[1] | ITIL -Information Technology Infrastructure Library, v.3.

C) **Incident Investigation & Diagnosis** – this stage includes gathering information regarding incident and conducting analysis to determine its causes. Evidence gathered during investigation phase are used for incident resolution, but later may be also required during legal proceedings. That is why for major incidents, or those for which there is suspicion that they were caused by illegal activities, gathering of evidence has to be clearly documented and conducted according to the procedures developed in compliance with existing law regulations. As this can be time consuming, this may create a challenge in the critical infrastructure environment where the priority will be to restore processes important to the safety of large groups of people. In the end, it may be easier to create a snap shot of the state of the system in the time of incident for the future analysis, and directly proceed with the system restoration from the backups than try to conduct a full diagnosis in the first place.

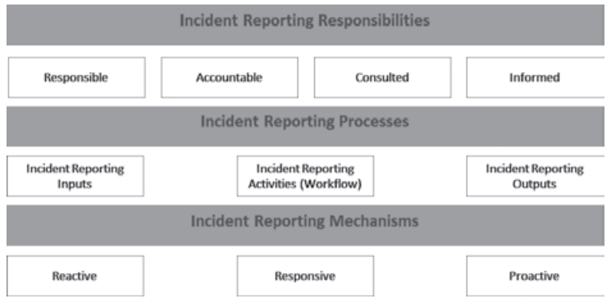
D) **Incident Resolution & Recovery** – this stage usually includes containment of the problem, eradication and finally recovery of the disturbed assets. Containment is usually required in malware-related incidents for the protection of other assets and resources. In other kind of attacks, conducted actions may include disconnecting particular system from the outer network or switching to the secondary operation centre. In case of incidents that are an effect of a human error or badly defined processes, the containment may be limited or not needed.

E) **Incident Closure** – covers mostly administrative actions which are treated as a priority in the previous stages. This includes documentation, but may also cover a detailed analysis of roots of the incident and planning on implementation of required mitigation measures. Depending on the chosen model, this stage may also include reporting of the security incident to the responsible authorities, on which the further parts of this article will be focused.

3. Incident reporting in the context of Protection of Critical Infrastructure

Many of European MS, who are more mature in the area of Critical Infrastructure protection, have already implemented an obligatory reporting of security incidents by CI operators on the national level. As some corrections in the overall approach may still be required (range of reported information, reporting parameters), the overall additional effort for aligning existing processes with the EU requirements should not be significant. Also, already successfully implemented models should be thoughtfully analysed from the point of view of its pros and cons, and considered for implementation by less mature countries.

The table below describes one of the possible approaches to the description of incident reporting process parameters:



Incident Reporting Responsibilities

Responsible | Accountable | Consulted | Informed

Incident Reporting Processes

Incident Reporting Inputs | Incident Reporting Activities (Workflow) | Incident Reporting Outputs

Incident Reporting Mechanisms

Reactive | Responsive | Proactive

Tabele 1: Approaches to description of incident reporting process parameters.

Three major areas which define the targeted incident reporting framework include:

▶ Incident Reporting Responsibilities – the definition of RACI; identification of who should report to whom, and clear definition of the roles in the incident reporting process:
–Who needs to report an incident?

- Who is responsible, accountable, consulted and informed in an incident reporting process?
- To whom Member States/critical infrastructure operators should report a security incident?

▶ Incident Reporting Processes – the definition of inputs and outputs, as well as the incident reporting workflow; establishing a repeatable and standardised procedure:

- What is the definition of an Incident?
- What are the criteria for initiating an incident reporting process?
- What are the different incident categories?
- What are the rules for incident priorities?
- What are the necessary functions of the incident reporting framework?
- What is the information content of security incident reports?
- What is the output of an incident reporting process?

▶ Incident Reporting Mechanisms – the definition of incident reporting mechanisms; defining a scope and level of involvement in incident handling and information sharing across market operators:

- How do Member States/critical infrastructure operators report an incident?
- What is the frequency and pace of incident reporting?
- What are the response mechanisms after reporting an incident?

4. Main challenges in incident reporting

Successful introduction of incident reporting process between CI operators and government institutions requires not only proper regulations in place but also a mutual understanding of needs, problems and fears. There are numerous reasons why CI operators may not be eager to share information regarding security incidents. First of all, a lot of those organisations are commercial companies – if information about security incident would become a noisy affair it could have an impact on the company's reputation and trust of its customers. Therefore, providing this kind of information when it is not absolutely necessary may be considered by stakeholders as acting to the detriment of the company. Moreover, in the end, CI operators are responsible for the safety operations of its infrastructure. As most of them are large companies with mature processes, they believe risk management cycle they already have in place is sufficient to protect them from existing threats – including cyber-related. Therefore, they consider additional interest of government institutions as a problem rather than help, where sharing of information may work as a trigger for development of new regulations, which will create additional compliance effort and costs. The other important aspect is where the incidents have to be reported. This is especially important when operator's headquarters are in a different Member State than the one where incident occurred. Building a trust between CI operators and national administration requires time and communication of goals of the programme and common benefits gained through the implementation of incident reporting. Communication provided from government institution's side should include at least answers to the following questions:

1) Who is obliged to report the incidents?

As many CI sectors are already covered by other mature and detailed regulations, it seems now that upcoming NIS directive may in the end cover only some of CI operators[2]. Also, an ENISA ICS/SCADA security maturity assessment conducted in the middle of 2015 provided an important observation – although European EPCIP has been established a couple of years ago, not every EU MS managed to identify its CI assets and operators as of yet[3]. As this naturally has to be the first step of the organised approach to the CI protection (followed-up, among others, with establishment of communications channels, sector specific public-private partnership groups, etc.), there is a small chance that countries which were not able to build any basis for its CIP programme will be able to implement the incident reporting process anytime soon. For more mature countries that have already been able to build community around CI protection, defining a list of entities obliged to the reporting and development of communication channels dedicated to this purpose will be much easier – as both CI operators and responsible government institutions already know each other, and it will be much easier for them to develop a commonly acceptable, efficient methods of reporting. A valuable information regarding possible approaches to identification country's CI assets can be found in: "Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication networks." ENISA, 2014.

2) What has to be reported?

SIEM and other security systems within large organisations can identify hundreds of security alerts per day from which only a limited number will be classified as security incident. Also, only a very limited number of events will be important from the perspective of the wide CI protection programme. The common criteria which would later have to be implemented into the incident classification processes of CI operators have to be developed to support CI operators in the decision if particular incident should be reported or not. Generally, it is important that entities responsible for CI protection on national or EU level understand the most probable source/root of the incident, nature of attacks, including methods which were used by attackers, related impact (but also the potential impact which an incident could have if implemented security measures did not play their roles), how the attack was detected and mitigated. Especially valuable are reports regarding incidents which unveil new means of attack or those which could have (or actually had) a significant impact on the CI operations.

For the less significant incidents, a detailed reporting does not seem to be necessary, however, some accumulated security metrics like volume of incidents in division to categories will be obviously useful from the perspective of trends' monitoring.

3) Why is incident reporting required?

One on the most important communication requirements for achieving an efficient incident reporting system is to ensure understanding of the purpose of this obligation by CI operators and benefits they will gain from their contribution to the CIP programmes. Access to the real information regarding the nature of the incident allows government institutions to develop supporting measures focused on bringing real value to the operators. Moreover, as security should not be considered as one of the competition factors, CI operators should be aware that providing information regarding threats they come across means obtaining similar knowledge from other operators. This will allow them to implement appropriate security measures in advance. Results from the research performed by EY[4] together with 1.755 organisations worldwide in the year 2015 may indicate that in many cases organisations are still not sufficiently effective in fighting against cyberthreats. More than one third of respondents think it is unlikely for their organisation to identify a sophisticated cyberattack and only seven percent of the organisations claim to have a very mature, robust incident response program. Moreover, in case of 14 percent of responders incident response capability was not even created. Also, one fifth of organisations was not able to estimate the total financial damage related to cyber incidents in the last 12 months. Thus, joint efforts

[2] | The Network and Information Security Directive – who is in and who is out?, Luke Scanlon, Out-Law.com.

[3] | Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors, ENISA, 2015.

[4] | EY's Global Information Security Survey 2015, Ernst & Young, 2015.

may be required in order to help organisations and governments better defend their key assets in the future. Involvement of national authorities in the process gives a high chance of maintaining anonymity of organisation which was subject to the attack and maximum limitation of the group of people who have access to information about the particular incident. Therefore, it is much less probable that the information will be misused.

4) **How reporting should be conducted?**

Currently, many of CI operators are not prepared to the incident reporting implementation from both operational and organisational perspective. When EU MS will implement NIS Directive with local regulations, they will define requirements towards incident reporting. CI operators will have fulfil these requirements. To support these processes, proper organisation and technical solutions will have to be implemented. The responsible organisation units will be originating usually from a higher level of government administration, as they will be dealing with authorities. From operating perspective, efficient methods will have to be developed by operators to: monitor OT and IT assets, detect and correctly classify security incidents, mechanisms for processing and analysis of gathered information, and finally to provide required information in a secured way. Recommendations towards defining and implementation of incident reporting processes on company level will be described in future articles from the series.

5. Conclusion

This article is the first of the series and it is only a short introduction to a much broader subject. However, based only on some of the most basics questions we have a unanimous conclusion that successful implementation of a real incident reporting and information sharing will take creation of good frames, serious decisions, officials support and time to become fully operational. Moreover, it is worth highlighting that creating coordinated incident reporting process both on the EU/governments and organisational level is only one of the initial steps which have be taken in order to build an effective system allowing to defend against cyberthreats. Further questions related to obligatory reporting, specific data gathering, analysis and further exchange in order to increase the security of the organisations need to be answered. ■

ANALYSIS

GATHERING IDENTIFIER SYSTEM AND CYBERATTACK THREAT INTELLIGENCE

DAVE PISCITELLO
has been involved in Internet technology for over 40 years, and serves presently as Vice President, Security and ICT Coordination at ICANN. He regularly collaborates with the information security, operations, and law enforcement communities on a diverse range of security issues related to the Domain Name System and domain name registration processes, including phishing, spam, botnets, DDoS attacks, domain hijacking and registration abuses.
Mr Piscitello's research includes proxy and private domain registration abuse, REST-based Internet directory services, domain seizures and DNS abuse investigative techniques. Dave has authored books on internet protocols, remote access and Voice over Internet Protocol Security (April 2006). He publishes articles regularly on Internet security, DNS, antiphishing, malware, Internet policy and privacy.

1. Introduction

The cyberattack threat landscape is extensive. Financially motivated attacks such as fraud or the distribution of illicit or counterfeit goods are among the most prevalent. Commercial or state-sponsored espionage figure prominently as well. Conflict-purposed threats, from terrorist radicalization and recruitment to state-sponsored aggression, are no longer merely story lines for suspense or action films. Gathering information or "intelligence" to detect or mitigate these or other cyberattacks is a daunting process. Threat actors or conspirators often operate pan-globally. The resources they use to execute threats are pan-global as well, and the numbers of assets these actors usurp or employ for a given attack may count in the hundreds of thousands or even millions. While the advantages seem to be overwhelming align on the side of the attackers, threat responders or investigators have one advantage: attackers must use the Internet to reach their targets or victims, and responders can gather information that reveals how they are using the Internet, where, and to what is a purpose.

Internet identifiers – domain names, Internet addresses and associated registration or reputation data – are some of the most useful and informative data which threat responders can monitor, collect and analyse. We describe the data sets that can be collected when we investigate cyberattacks. We identify examples of open source or commercial tools to collect this data and provide examples of how it can be automated to facilitate collection and analysis.

2. Identifier Systems

Three Identifier systems play key roles in nearly all forms of Internet-based commerce, collaboration and content publication or distribution.

Internet Protocol (IP) addresses identify networks and individual host computers. They loosely correspond to streets and building numbers in the real world. The prominent version of IP addresses in use today is IP version 4 (IPv4), a 32-bit address typically represented in "dotted-decimal" notation, e.g., 192.168.0.1. The IPv4 address space is fully allocated and investigators will increasingly encounter a new version 6 (IPv6), which is 128 bits long, represented in "colon-hexadecimal" format with leading zero-suppression, e.g., 2a00:1450:4001:800::1013.

Autonomous System Numbers (ASN) are 16- or 32-bit numbers that identify network operators (typically, large Internet Access or Service Providers, ISPs) or content hosting operators. While ASNs are most commonly associated with global routing by technical staff, for purposes of cyberattack investigations, we find it helpful to describe ASNs as identifying the Internet's "neighbourhoods."

Domain Names provide case-insensitive, user-friendly means to identify hosts or organisations. Domain names are delegated from a *Top Level Domain (TLD)* to a party through a registration process. Historically, domain names have been represented using letters, digits and hyphens, but now they may be registered in native languages or scripts that use Unicode characters[1], including Arabic script, Cyrillic, Hangul, Thai, etc.

Two other identifier systems may be relevant to investigators. Port numbers are identifiers that identify a process or a service that is operated on a host computer[2]. *Protocol parameters* are identifiers of particular Internet protocols such as TCP, UDP, ICMP, etc.[3].

These identifiers, combined, often provide the geo-location of a threat asset, clues to the alleged operator of an asset, and some idea of how the asset is being used. The identifiers are also necessary to probe deeper into the means used to conduct the attack, e.g., perhaps content hosted at a web site, or a malicious electronic mail.

Associated registration data for these identifiers can provide point of contact information of operators.

3. Identifier Systems Dossier Composition

Gathering information associated with a cyberattack often follows a classic forensic or investigative process of identifying means, motive and opportunity. Here, we will explain how one can compile a dossier of information using an investigation of an alleged illegal pharmaceutical web page as an example; however, the methodology and, in particular, the means and information we gather are generally appropriate for any of the aforementioned types of attacks.

In our example, we begin with a domain name that we extracted from a (URL[4]) that we found in a spam email message that promotes the sale of pharmaceutical drugs without prescription. Specifically, we extracted the domain name smarthealingstore.ru from hxxp://hctiwiga.smarthealingstore.ru/[5].

We will begin our investigation by asking, "what is the IP address associated with this domain name?"

4. Gather Resource Records From The Domain Name System

We can query the DNS, Domain Name System[6], to determine the IP address and many other esource records associated with this domain name using any of several command line utilities – host[7], dig[8], nslookup[9]– that are available for most general purpose operating systems, or from hundreds of web sites that provide the equivalent name resolution service. Here, we use several dig commands to obtain address, name server information, and because we were dealing with spam, we obtain mail exchange resource records as well:

```
$ dig A smarthealingstore.ru +nocomment

; <<>> DiG 9.8.3-P1 <<>> A smarthealingstore.ru +nocomment
;; global options: +cmd
;smarthealingstore.ru.        IN    A
smarthealingstore.ru.   332   IN    A     91.200.12.32
smarthealingstore.ru.   514   IN    NS    ns2.smarthealingstore.ru.
smarthealingstore.ru.   514   IN    NS    ns1.smarthealingstore.ru.

ns1.smarthealingstore.ru. 344563 IN  A     211.110.14.21
ns2.smarthealingstore.ru. 344563 IN  A     180.149.245.175
;; Query time: 43 msec
;; SERVER: 10.47.11.34#53(10.47.11.34)
;; WHEN: Mon Feb 22 12:30:35 2016
;; MSG SIZE rcvd: 122

$ dig mx smarthealingstore.ru +nocomment

; <<>> DiG 9.8.3-P1 <<>> mx smarthealingstore.ru +nocomment
;; global options: +cmd
;smarthealingstore.ru.        IN    MX
smarthealingstore.ru.   351   IN    MX    10 mail.smarthealingstore.ru.
smarthealingstore.ru.   350   IN    NS    ns2.smarthealingstore.ru.
smarthealingstore.ru.   350   IN    NS    ns1.smarthealingstore.ru.
mail.smarthealingstore.ru.  377 IN    A     91.200.12.32
ns2.smarthealingstore.ru. 266404 IN  A     180.149.245.175
ns1.smarthealingstore.ru. 266404 IN  A     211.110.14.21
;; Query time: 48 msec
;; SERVER: 10.47.11.34#53(10.47.11.34)
;; WHEN: Tue Feb 23 10:13:14 2016
;; MSG SIZE rcvd: 143
```

[1] | Internet Corporation for Assigned Names and Numbers (ICANN). Internationalized Domain Names, [online] https://www.icann.org/resources/pages/idn-2012-02-25-en.

[2] | Internet Assigned Numbers Authority (IANA). Service Name and Transport Protocol Port Number Registry, [online] http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

[3] | Internet Assigned Numbers Authority (IANA). Protocol Registries, [online] https://www.iana.org/protocols.

[4] | Computer Hope. URL, [online] http://www.computerhope.com/jargon/u/url.htm.

[5] | When sharing hyperlinks, investigators substitute "hxxp" for "http" in correspondence to protect recipients from accidentally visiting a malicious hyperlink.

[6] | Dyn DNS. What is the Domain Name System (DNS)? , [online] http://whatismyipaddress.com/dns.

[7] | UnixRef.com. The Host Command, [online] http://www.unixref.com/guides/host-guide.php.

[8] | Linux.com. Check Your DNS Records with dig, [online] http://www.linux.com/learn/tutorials/442431-check-your-dns-records-with-dig.

[9] | Microsoft Technet. nslookup, [online] https://technet.microsoft.com/en-us/library/bb490950.aspx.

Many programming languages have DNS resolver libraries (e.g., Net::DNS[10] for PERL, adns[11] for C/C++). These are often more efficient to use when investigators must gather data from very long lists of domain names. The dnspython[12] package for the Python language developers is an example of such libraries. Performing a lookup for an address record using dnspython is illustrated below:

```
# accept both a domain name and URL from command line
parser = argparse.ArgumentParser(description=’Identifier Systems Information
Gathering Tool’)
parser.add _ argument(‘-d’, ‘-fqdn’, help=’Domain (FQDN)’, required=True)
parser.add _ argument(‘-u’, ‘-yourl’, help=’Hyperlink (URL)’, required=True)
args = vars(parser.parse _ args())

domain = args[‘fqdn’]
myurl = args[‘yourl’]
# get A records
with open(‘arecord’, ‘w’) as f:
# dnspython equivalent of “dig A +authority domain
resolver = dns.resolver.Resolver()
resolver.nameservers = [‘8.8.8.8’, ‘8.8.4.4’]
# using google open resolvers
try:
answers = resolver.query(domain, ‘A’)
f.write(‘Ipv4 records for query qname: ‘)
f.write(‘\n %s’ % answers.rrset)
except dns.resolver.NoAnswer:
f.write((‘\n No answer for %s’ % domain))
except dns.exception.DNSException:
f.write(‘\n DNS Exception while processing address query’)
except dns.resolver.NXDOMAIN:
f.write((‘\n NXDOMAIN for %s’ % domain))
```

Irrespective of which of these DNS toolkits we use, we now have several “leads” – identifiers – to investigate further.

5. Follow Leads: The Bases For Further Investigation

The questions we want to attempt to answer with our leads include:

- Who has registered this domain name?
- Who was assigned to this IP address block?
- Who is announcing it to the Internet?
- What is the physical geo-location of the host computer, name server(s), and mail exchanger?
- What other domains can we find on the IP addresses we have identified?
- Is there anything hosted at the IP addresses we have identified, which may be seemingly suspicious or known/confirmed to be malicious?

Answers to these kinds of questions can reveal a broader attack surface (many more domain names and IP addresses) than it is immediately obvious from any single IP address[13]. The answers may identify parties to a conspiracy. These lines of questioning are very similar to good investigators who would ask as they study a real world crime scene, collect physical evidence, question possible witnesses, review video tapes or more.

6. Identifying Persons Of Interest: Domain And Address Registration Data (Whois)

Individuals or organisations normally must register domain names and IP address blocks before use Registration details are being collected during that registration processes. Some or all of this registration data may be published, depending on prevailing privacy regulations. Investigators can use an ubiquitously available query service called WHOIS[14] to obtain publicly available data. Some of the registration data that are relevant to our investigation can be obtained by using the whois[15, 16], command:

```
$ whois smarthealingstore.ru
% By submitting a query to RIPN’s Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).

domain: SMARTHEALINGSTORE.RU
nserver: ns1.smarthealingstore.ru. 211.110.14.21
nserver: ns2.smarthealingstore.ru. 180.149.245.175
state: REGISTERED, DELEGATED, VERIFIED
person: Private Person
registrar: R01-RU
admin-contact: https://partner.r01.ru/contact _ admin.khtml
created: 2016.02.03
paid-till: 2017.02.03
free-date: 2017.03.06
source: TCI

Last updated on 2016.02.23 17:31:32 MSK
```

The response reveals operational data about the registered domain name. Note that it does not reveal any point of contact information that might lead us to a party which we might investigate. Even in circumstances where prevailing regulations or contracts permit the disclosure of point of contact information, investigators must expect that cyberattackers might have submitted false or inaccurate information. The operational registration data, however, are trustworthy and may be useful for identifying hosting operators, and even inaccurate data may be used to associate multiple registrations with a particular cyberattack or a gang. Investigators also make use of a commercial service such as Domain Tools[17] or CyberTOOLBELT[18] that offer historical data and other advanced multi-record search capabilities.

IP address block registrations are typically more accurate, if detailed assignment information is present. IP address resources are commonly allocated to global network operators or large hosting providers and then delegated further to customers. Investigators can use the autonomous system

[10] | Academy of Finland. 2012. Computer and Information Science. Background report to State of Scientific Research in Finland 2012 Report. http://www.aka.fi/fi/tiedepoliittinen-toiminta/tieteen-tila/aiemmat-arvioinnit/tieteen-tila-2012/

[11] | GNU.org. GNU adns, [online] http://www.gnu.org/software/adns/.

[12] | dnspython.org. A DNS toolkit for python, [online] http://www.dnspython.org/.

[13] | Piscitello. David. Identifying Cybercriminals: Is an IP Address Sufficient? , [online] http://www.securityskeptic.com/2016/02/identifying-cybercriminals-is-an-ip-address-sufficient.html.

[14] | Internet Corporation for Assigned Names and Numbers (ICANN). About WHOIS, [online] https://whois.icann.org/en/about-whois.

[15] | Microsoft Technet. Whois v1.1.13. https://technet.microsoft.com/en-us/sysinternals/whois.aspx.

[16] | Computer Hope. Linux and UNIX whois command, [online] http://www.computerhope.com/unix/uwhois.htm.

[17] | DomainTools. DomainTools WHOIS, [online] https://whois.domaintools.com.

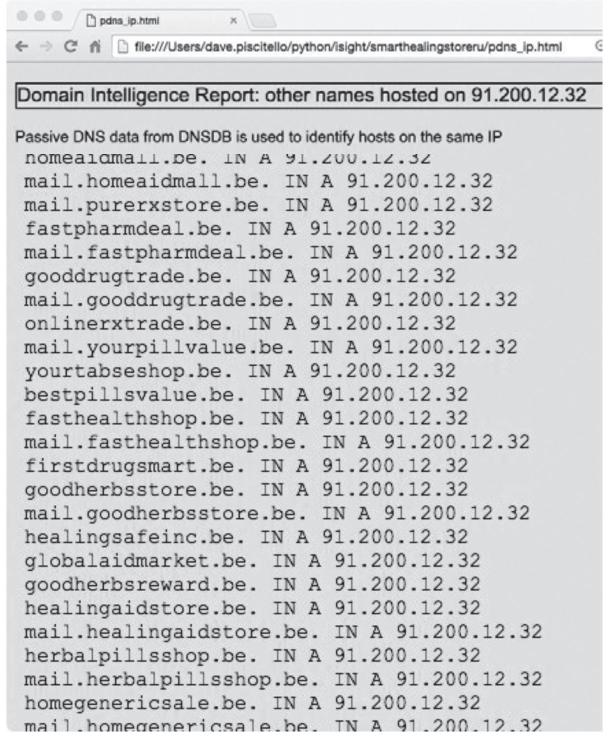
[18] | CyberTOOLBELT, [online] https://www.cybertoolbelt.com/.

numbers and address blocks of these operators or customers to geo-locate the hosting locations of web, DNS, or mail servers associated with the domain name that is the subject of the investigation, and to query the RIPE NCC RIPEstats[19] databases or Hurricane Electric BGP Toolkit[20] using ASNs or IP addresses to obtain routing and abuse data that may be pertinent to the investigation.

They can also more reliably contact operators using the registration data provided for IP WHOIS rather than domain name WHOIS point of contact data.

7. Canvass Crime Scenes And Neighbourhoods

All Internet users query the DNS hundreds or thousands of times each day. By collecting the queries and responses from thousands of servers that provide name resolution, and amassing them into database repositories, we can make a query service available that investigators can use to determine relationships among domain names, name resolution servers, and IP addresses. Passive DNS Replication (PDNS[21]) services often help investigators to identify a cyberattacker's resources and may be useful to map out the infrastructure associated with a cyberattack. Several commercial, consulting[22] and research[23] organisations offer Passive DNS replication services. These service operators provide application programming interfaces and libraries to facilitate automation. For example, we use the script dnsdb-query[24] to the DNSDB[25] passive DNS replication service using the IP address 91.200.12.32 from our earlier dig query,which shows that many other domain names are hosted at this address. Figure 1 shows a partial enumeration of replicated DNS data:


pdns_ip.html
file:///Users/dave.piscitello/python/isight/smarthealingstoreru/pdns_ip.html

Domain Intelligence Report: other names hosted on 91.200.12.32

Passive DNS data from DNSDB is used to identify hosts on the same IP

```
homeaidmall.be. IN A 91.200.12.32
mail.homeaidmall.be. IN A 91.200.12.32
mail.purerxstore.be. IN A 91.200.12.32
fastpharmdeal.be. IN A 91.200.12.32
mail.fastpharmdeal.be. IN A 91.200.12.32
gooddrugtrade.be. IN A 91.200.12.32
mail.gooddrugtrade.be. IN A 91.200.12.32
onlinerxtrade.be. IN A 91.200.12.32
mail.yourpillvalue.be. IN A 91.200.12.32
yourtabseshop.be. IN A 91.200.12.32
bestpillsvalue.be. IN A 91.200.12.32
fasthealthshop.be. IN A 91.200.12.32
mail.fasthealthshop.be. IN A 91.200.12.32
firstdrugsmart.be. IN A 91.200.12.32
goodherbsstore.be. IN A 91.200.12.32
mail.goodherbsstore.be. IN A 91.200.12.32
healingsafeinc.be. IN A 91.200.12.32
globalaidmarket.be. IN A 91.200.12.32
goodherbsreward.be. IN A 91.200.12.32
healingaidstore.be. IN A 91.200.12.32
mail.healingaidstore.be. IN A 91.200.12.32
herbalpillsshop.be. IN A 91.200.12.32
mail.herbalpillsshop.be. IN A 91.200.12.32
homegenericsale.be. IN A 91.200.12.32
mail.homegenericsale.be. IN A 91.200.12.32
```

Figure 1: Passive DNS Enumeration Of A Suspicious IP Address.

With enumerations of this kind, we look for domains with similar string properties to our initial domain of interest, e.g., use of copyrighted brand, keyword, or algorithmic similarity. Here, we have found hundreds of domain names with strings associated with herbal remedies or pharmaceuticals. They are registered across many top level domains (747 in .be, 89 in .eu, 106 in .in, 77 in .nl, and 9855 in .ru). Now, investigators have approximately 10,000 domains that they can try to associate with the initial spam campaign complaint. Using automated methods, investigators can repeat the DNS and Whois queries previously explained to map out this spammer's infrastructure.

[19] | RIPE NCC. RIPEstats – Internet Measurements and Analysis, [online] https://stats.ripe.net.

[20] | Hurricane Electric. BGP Toolkit, [online] http://bgp.he.net/.

[21] | Weimer. Florian. Passive DNS Replication, [online] http://www.enyo.de/fw/software/dnslogger/first2005-paper.pdf.

[22] | BFK edv-consulting GmbH. Passive DNS Replication, [online] https://www.bfk.de/bfk_dnslogger.html.

[23] | Virustotal.com. VirusTotal += Passive DNS replication, [online] http://blog.virustotal.com/2013/04/virustotal-passive-dns-replication.html.

[24] | Farsight Security. Inc. DNSDB API, [online] https://api.dnsdb.info/.

[25] | Farsight Security. Inc. Welcome to DNSDB, [online] https://www.dnsdb.info/.

8. Collect Evidence From The Cyber Crime Scene

Collecting evidence in a cyber investigation typically involves gathering information from multiple hosting locations or traffic origins that span several legal jurisdictions. Investigators can often collect information such as web or file sharing site content by using methods that replicate how a victim or recruit would access such sites. For the domain name smarthealingstore.ru, investigators might suspect that the criminal activity involves hosted web content, so they might use command tools such as curl[26] or wget[27], scripts such as peepingtom[28], or web site copying software such as HTTrack[29] to download entire web or site's files content safely from suspicious domains or IP addresses, without executing scripts or other executable content that may be hosted at these locations.

Once downloaded, investigators can use a forensic tool like Bulk Extractor[30], The Harvester[31] or FOCA[32] to extract information relevant to our investigation. Basing on the content investigators would gather at smarthealingstore.ru hyperlinks, using these tools, they would determine that smarthealingstore.ru and many of the associated domains, they discovered using passive DNS replication queries, are affiliate web sites that promote the sale of a wide variety of pharmaceutical drugs without prescription.

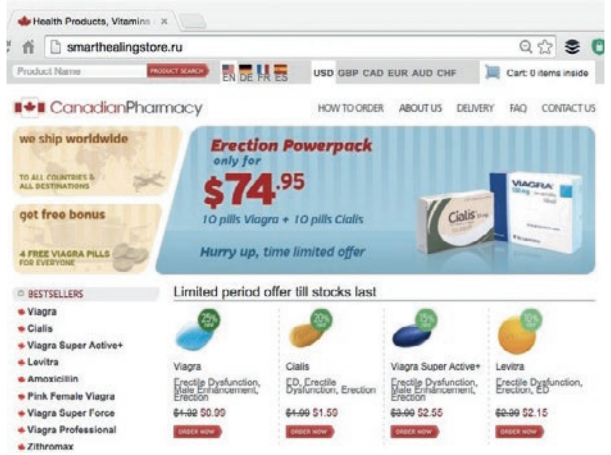


Figure 2: Example of an Illegal Pharmaceutical Merchant Web Page.

Figure 2 illustrates the discovered merchant page, as a hosted one. Investigators would likely continue to examine their accumulated content and metadata, and pursue suspects using this data. They may use this data as arguments in general, as well as, social media searches as means to learn about suspects' friends, activities or location. Persistent analysis of the data they would accumulate through these efforts often yield physical world leads, where investigators can use traditional police investigatory methods to zero in on suspected conspirators, gather further evidence, coordinate across jurisdictions (where necessary) with the goal of apprehending and prosecuting the offenders.

9. Manage Malicious Executables During Investigations

Only a small fraction of investigators have the kind of forensic analysis expertise that is necessary to inspect hyperlinks or to reverse engineer malicious executables (malware). Investigators can rely on cloud-based malware or URL analysis services such as VirusTotal[33] , URLquery[34], Wepawet[35], or

[26] | Computer Hope. Linux and UNIX curl command, [online] http://www.computerhope.com/unix/curl.htm.

[27] | Computer Hope. Linux and UNIX wget command, [online] http://www.computerhope.com/unix/wget.htm.

[28] | Piscitello. David. Get Aquainted with a peepingtom? You bet. , [online] http://www.securityskeptic.com/2014/10/get-acquainted-with-a-peepingtom-you-bet.html.

[29] | HTTrack.com. HTTrack Website Copier, [online] https://www.httrack.com/.

[30] | forensicswiki.org. Bulk Extractor, [online] http://www.forensicswiki.org/wiki/Bulk_extractor.

[31] | Google. Inc. The Harvester, [online] https://code.google.com/archive/p/theharvester/.

[32] | Eleven Paths. Fingerprinting Organizations with Collected Archives (FOCA) , [online] https://www.elevenpaths.com/labstools/foca/.

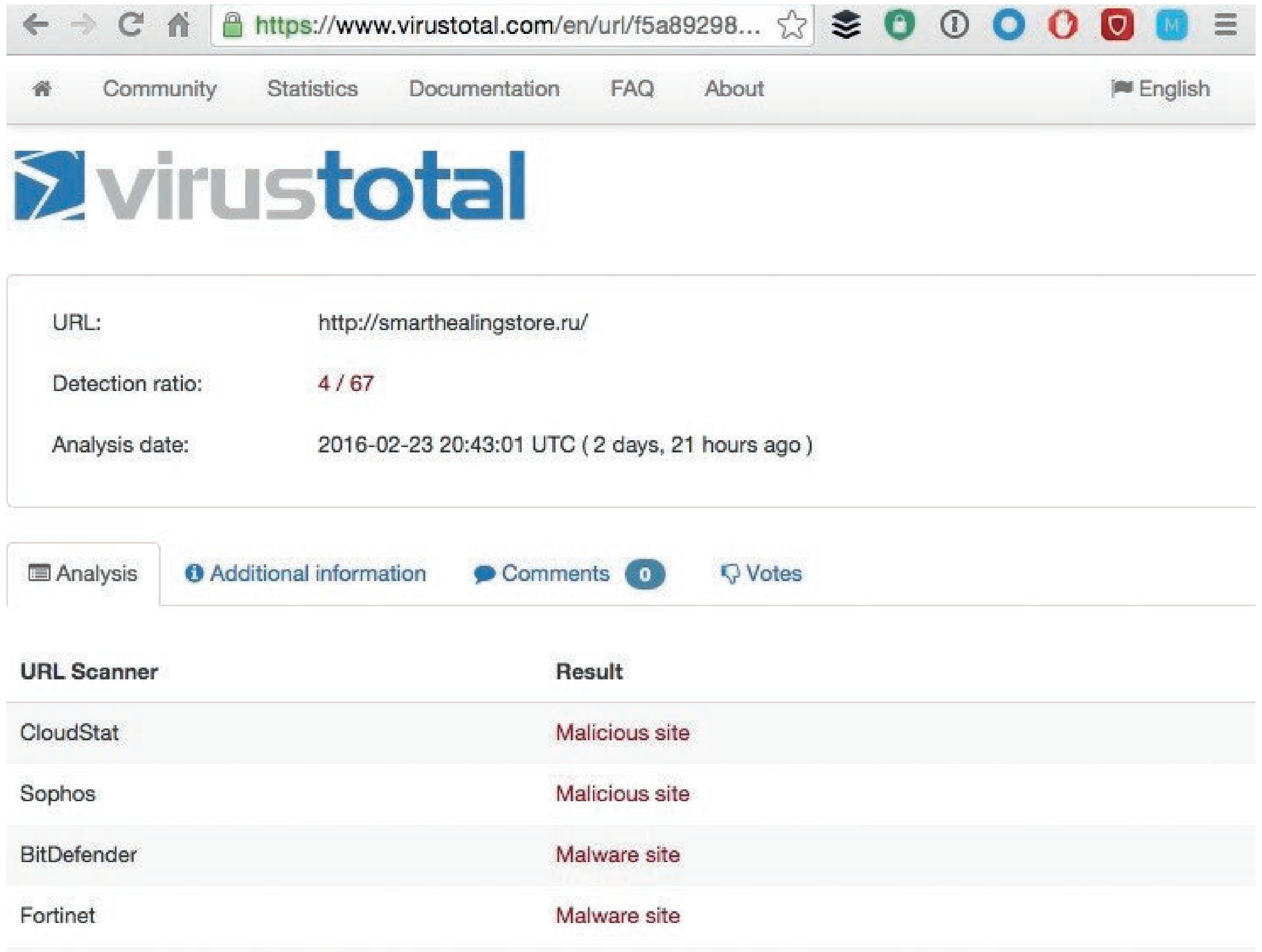
[33] | Virus Total. Analyze Suspicious files and URLs, [online] https://www.virustotal.com/.

[34] | URLquery service, [online] http://urlquery.net.

[35] | ISEClab.org, [online] Wepawet - a platform for the analysis of web-based threats. https://wepawet.iseclab.org/.

Anubis[36] for these kinds of analyses. Investigators can upload suspected malware samples or submit URLs for inspection. These services also maintain a historical database of a content or hyperlinks they have analysed, so both trusted malware sample sharing and fast reporting of previously submitted samples or URLs are available.

Figure 3 shows the summary report of findings for smarthealingstore.ru's IP address:



URL: http://smarthealingstore.ru/

Detection ratio: 4 / 67

Analysis date: 2016-02-23 20:43:01 UTC (2 days, 21 hours ago)

URL Scanner	Result
CloudStat	Malicious site
Sophos	Malicious site
BitDefender	Malware site
Fortinet	Malware site

Figure 3: Example of Summary Report Of URL Analysis.

10. Create Dossiers Or Summary Reports

Many of the tools discussed in this article provide programming APIs. They can be automated along with the DNS, WHOIS, PDNS, or RIPEstats query results to create per domain or multi-domain summary reports using a programming languages like python or PERL. For example, one might use the following packages available for python to quickly develop a reporting script:

Developer code	Location	Comment
dns.resolver	http://www.dnspython.org/examples.html	Domain name resolution
publicsuffix	https://pypi.python.org/pypi/publicsuffix/	Name parsing
json2html	https://pypi.python.org/pypi/json2html/	Json output formatting
pythonwhois	http://cryto.net/pythonwhois/	Domain whois client
ipwhois	http://www.admon.org/networking/query-ip-whois-info-in-python/	IP whos client
Geo-IP	http://api.hackertarget.com/geoip/?q=	Geo-location
RIPEstats	https://stat.ripe.net/data/as-routing-consistency/data.json?resource=	
ASN Routing		
	https://stat.ripe.net/data/announced-prefixes/data.json?resource=	Announced prefixes
	https://stat.ripe.net/data/network-info/data.json?resource=	Network info
	https://stat.ripe.net/data/blacklist/data.json?resource=	
	Blacklists	
dnsdb-query	https://api.dnsdb.info/	Passive DNS replication
isthisIPbad.py	https://github.com/jgamblin/isthisipbad	Multiple reputation checks

11. Avoid Collateral Harm To Other Investigations

A given cyberattack has the potential to victimize or harm individuals or organisations in nearly every corner of the Internet. It is highly likely that others are also investigating any domain name or IP address identified during an investigation. Investigators should also, where possible, use trusted communications channels to share intelligence in order to avoid interfering or disrupting ongoing investigations to avoid collateral harm, when they take action to disrupt or mitigate cyberattacks to avoid collateral harm[37,38,39].

12. Final Remarks

The methods to investigate a complaint of an online illegal pharmaceutical operation illustrated here are representative of how many cyberattack investigations proceed, but there are clearly attack-specific considerations that are not easily generalised. They hopefully serve for the intended purpose of this article.

Mapping a cyberattacker's infrastructure requires constant monitoring as the infrastructure may routinely and rapidly change. Investigators should iteratively gather the intelligence which we describe here to get a fuller picture of the attacker's resources and analyse how they are adapting their infrastructure to evade detection or avoid dismantling. For example, during the course of monitoring our smarthealingstore.ru domain, the IP addresses, where smarthealingstore.ru was hosted, changed several times.

If you choose to try some of the techniques presented here, your findings may be different from what is presented here. Or you may find that your queries will yield "no result" or "not found," which is possibly an indication that some investigator succeeded in suspending or dismantling these illegal activities. ■

[36] | ISEClab.org. Anubis – Malware Analysis for Malicious Binaries, [online] https://anubis.iseclab.org/.

[37] | Internet Corporation for Assigned Names and Numbers (ICANN), The value of assessing collateral damage before requesting a domain seizure, [online] https://www.icann.org/news/blog/the-value-of-assessing-collateral-damage-before-requesting-a-domain-seizure.

[38] | Piscitello, David. Is Jotform a poster child for domain shutdown overkill, [online] http://www.securityskeptic.com/2012/02/is-jotform-a-poster-child-for-domain-shutdown-overkill.html.

[39] | Dittrich, David, The Honeynet Project. Thoughts on the Microsoft's Operation b71, [online] http://www.honeynet.org/node/830.

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 sybersecurity. 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.

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

PRICING OF THE ANNUAL SUBSCRIPTION (4 ISSUES)

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

Electronic edition: € 199
excluding VAT, including handling

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

CONTACT INFORMATION

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

BANKING INFORMATION

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

THE ECJ IS 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