THE CROSS-BORDER CRITICAL INFORMATION INFRASTRUCTURE (CII) AND THE OPERATOR'S RESPONSIBILITIES. CASE STUDY

Engineer Ștefan-Gabriel GEORGESCU, PhD student*

Abstract: *Threats to our critical services nowadays are likely to emerge from the connected information infrastructure, and also include critical services located outside national borders. These systems must be protected. This article discusses the role of the operator of a critical service in securing our information systems, focusing on the legal obligations and responsibilities. It outlines the list of duties of critical infrastructure operators and points out the cross-border aspects, thus far little explored in the literature. It begins by discussing the risks attached to cross-border critical information infrastructure (CII). It then provides an overview on the duties which the operator has to comply with in order to keep the systems safe. The costs of securing these systems are also addressed. The article (case of study) firstly argues for the benefit of raising awareness among citizens of who safeguards our daily lives, and secondly, urges the main actors to look at the legal aspects before connecting to cross-border infrastructure. Finally, it provides stimulus for policymakers in the field of cyber security.*

Keywords: *cyber-attacks; critical information infrastructure (CII); prevent disruption; national border; armed attack; cross-border dependencies; information itself; of critical infrastructures (CI); protecting critical systems; denial of service (DoS); and cyber-power.*

1. INTRODUCTION

Electricity grids, gas and water pipelines, and road, rail, air and waterway transportation are among the most important sectors which enable our everyday lives, making them more comfortable. These sectors form part of the so-called *critical infrastructure (CI)*. *Dependencies* and *interdependencies* with them can oftentimes only be realized once things do not work the way they are expected to work. All of a sudden, society experiences a blackout[1], forcing most of the population to stop working on their computers, or the sewage system breaks down, leading to the contamination of the surrounding environment[2].

Today, more than eighty percent of our critical activities are run by private operators and not by the state itself[3]. Rather than concerns about safety issues, the aspects which rule daily business life are first of all efficiency and also oftentimes competitiveness. This will need to change in times when society fears *cyber-attacks* against critical infrastructure assets[4].

Globalization has led to the intertwining of our networks, including information infrastructure

[1] A major blackout happened in December 2015 in Ukraine which is believed to be the first known case where a cyber attack takes down the energy network, see: http://www.telegraph.co.uk/technology/news/12082758/Ukrainian-blackout-blamed-on-cyber-attack-in-world-first.html and a U.S.-report https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 accessed 29 February 2016. There are other large blackouts to remember such as in 2014 in Bangladesh, the Philippines, Malta, Egypt, New Zealand and South Africa or in 2015 in Pakistan, The Netherlands and Turkey.

[2] In 2001 a former employee hacked into the sewage system of an Australian city, causing 800,000 litres of raw sewage to spill out into the local environment, contaminating to parks and rivers. See also http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, accessed 26th January 2017.

[3] NATO, The World in 2020 – Can NATO Protect Us? The Challenges to Critical Infrastructure, Conference Report, Brussels 2012, p. 11, available at http://www.natolibguides.info/ld.php?content_id=1675627, accessed 25 March 2017.

[4] See also Vytautas Butrimas, Thoughts on Possible Cyber security Misconceptions over the Security of the Energy Sector, 21st January 2017, http://www.hazar.org/analisdetail/analis/thoughts_on_possible_cybersecurity_ misconceptions_over_the_security _of_the_energy_sector_1276.aspx, accessed 24 March 2017.

*** University of Bucharest, Romania**
e-mail: stefan.georgescu@3nanosae.org

which may be located outside the national border. But while the systems become more and more efficient by being interconnecting, at the same time they become more dependent upon the information infrastructure and the threat level increases significantly.[5]

Safeguarding the information system behind the critical infrastructure is of vital importance, and a great number of regulatory schemes therefore place obligations on operators. These obligations might differ slightly depending on which country the operator is executing the tasks from. At the same time, incentives for the operator to fulfill the set of obligations can seldom be found in national laws.

This article aims to address how states safeguard their *critical information infrastructure (CII)* and *prevent disruption*. In particular, it will examine the obligations placed on the operator of CII, and the role of *financial investment in securing the systems*. Finally, it will ask whether more state action, including incentives, is needed to support operators in safeguarding our *information systems*.

The article serves to raise awareness among citizens of the challenges that the operators of critical information infrastructure face in their daily business. In addition to this, it addresses policymakers by presenting *thought-provoking information*. However, it does not attempt to deal with the questions of whether or when a cyber-attack against CIIs is considered an *armed attack*, or when self-defense according to Article 51 of the UN Charter applies.[6]

2. Critical Information Infrastructure (CII)

The term CII must have only evolved at about the same time that computers started to revolutionize our mechanical systems only a few decades ago. The meaning might oftentimes not be clear, and sometimes *critical information infrastructure (CII)* is not always approached as a distinct critical sector but rather as an integral part of a critical service.[7] National legal definitions of the term CII are few, but can be found, for example, in the Czech Act on Cyber Security and Change of Related Acts.[8]

Generally speaking, CII can be understood as a broad concept that designates both the *information itself (data flow)* and the channels through which information is created and conveyed (the computer networks).[9] According to this definition, examples of CII can be the telecommunication networks, the internet, or satellites, and examples of *critical infrastructures (CI)* are the financial sector (e.g. online banking, involving servers which are located cross-border), the transportation sector (aviation, rail, road, water), and the energy sector.

2.1. The known risks to cross-border critical information infrastructure (CII)

CII is a product of our competitive world, urging us to act faster, more efficiently and more precisely. But it is not the result of a wish to make our infrastructure safer. Today, most CI is computer controlled, and CI that is free or unaffected from interconnected systems is almost unimaginable.[10]

---

[5] See for example statement of US NSA Chief M. Rogers who says that it is only a matter of when, not if, a nation will experience destructive acts against critical infrastructure: http://www.securityweek.com/nsa-chief-worries-about-cyber-attack-us-infrastructure, accessed 24 March 2017.

[6] For more information on this question see Melzer, *Cyber warfare and International Law*, 2011, UNIDIR Resources, pp. 14-16, available at http://unidir .org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf, accessed 26th January 2017; Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law*, vol. 37, 1998-99; Condron, Getting it right: Protecting American Critical Infrastructure in Cyberspace, *Harvard Journal of Law & Technology*, Vol. 20, no. 2, spring 2007; Terry, *The War on Terror*, Rowman and Littlefield Publishers, UK 2013, p. 139 ff.; Schaller, *Internationale Sicherheit und Völkerrecht im Cyberspace, SWP-Studie*, Oktober 2014, Berlin, p. 18.

[7] K. Kaska and L. Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, NATO CCD COE, Tallinn 2016, p. 10f., available at https://ccdcoe.org/multimedia/regulating-cross-border-dependencies-critical-information-infrastructure.html, accessed 25 March 2017.

[8] §2 b) of the Czech Act on Cyber Security and Change of Related Acts (Act No. 181/2014 Coll., entry into force on 01 January 2015) defines CII as follows: 'Critical information infrastructure means an element or system of elements of the critical infrastructure in the sector of communication and information system within the field of cyber security.

[9] NATO Parliamentary Assembly, The Protection of Critical Infrastructures, doc. no. 162 CDS 07 E REV 1, para. 72, http://www.nato-pa.int/default.asp?SHORTCUT=1165, accessed 25 March 2017.

[10] See also Brunner, E. and M. Suter, International CIIP Handbook 2008/2009, p. 35, http://www.css.ethz.ch/publications/pdfs/CIIP-HB-08-09.pdf, accessed 22 February 2017.

Free trade agreements have played a defining role in interconnecting our critical services across borders. Common open markets like the EU have facilitated the interconnection of communication networks. In order to promote, for example, the free movement of goods, persons, services, and capital, the necessary infrastructure like road, rail and airways, servers, and undersea cables need to be interconnected, meaning that they will go beyond a state's border. These activities come at a price, and safety issues in particular consequently become much more challenging.[11]

The majority of risks that arise when locating a critical asset like information infrastructure within another state's territory are largely comparable to those risks faced by nationally hosted CI. The risks are mainly threefold: technological, financial and social.[12]

Effects reaching across borders can cause disruption of a system, as happened for example in 2014 in Bangladesh.[13] In this case, the electrical grid supplying Bangladesh with power from India failed due to a technical problem. This led to the failure of pumps in Bangladesh which were supposed to lift groundwater.[14] Given this, surprisingly little research has so far been done in the field of *cross-border dependencies* of CII. There is analysis of the interdependencies of infrastructures, but it mostly refers to those located within the same state, focusing on different regions within the same borders.[15]

This is striking given the age of globalization and in times when countries join crucial projects, for example, on cross-border electricity supply.[16] The lack of literature concerning these aspects could also be a sign that many people, both from the public and private sectors, work in walled-off structures where they deal with security issues as though they would not concern their neighbors or other countries. A study by the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE), *Regulating Cross-Border Dependencies of Critical Information Infrastructure*,[17] revealed that there are no discernible examples of legal and regulatory remedies to mitigate the risks arising from *cross-border CII.*

Determining which pieces of infrastructure are essential assets that are connected to an information infrastructure helps to forecast the potential impact of an incident, such as a *cyber-attack* targeting cross-border located information infrastructure. Kaska and Trinberg[18] found that there is a predominantly high degree of dependence on such cross-border information infrastructure, which can be highlighted as a critical weakness for the ICT and telecommunications sectors, the finance sector, and the energy supply, traffic and transportation sectors.[19] The media (print and broadcast) is substantially dependent on cross-border information infrastructure,[20] and other sectors including healthcare, water supply, government and administration, public and public order, and agriculture have been assessed as being dependent to some extent. Only a very small percentage of the participants of the study reported that some of

[11] Recent naval activity by Russian submarines near vital undersea cables is worrying because if Russia is planning to disrupt the global internet, repairing the undersea cyber infrastructure will be a challenging task; http://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html, accessed 04 March 2017.

[12] Kaska, Trinberg, *op. cit.,* p. 17f.

[13] See also http://www.npr.org/blogs/thetwo-way/2014/11/01/360656591/national-blackout-bangladesh-in-massive-power-outage, accessed 24 March 2017.

[14] Note, that the Bangladesh incident is not believed to be a cyber attack but a failure of the transmission lines, http://www.bbc.co.uk/news/world-asia-29869272, accessed 22 February 2017.

[15] See for example Metropolitan Washington Council of Governments, State of the Region Infrastructure Report 2015; B. Graves, *'The Critical Interdependence of Our Infrastructure'*, 28th January 2017, http://www.governing.com/blogs/view/gov-critical-interdependence-regional-infrastructure.html, accessed 29th January 2017; P. Cheng et al., Managing critical Infrastructure Interdependence through Economic Input-Output Methods, Journal of Infrastructure Systems, 2009, pp. 200-210; T.D. O'Rourke, *Critical Infrastructure, Interdependencies and Resilience*, The Bridge, vol. 37 no. 1, 2007, pp. 22-29.

[16] The Black Sea Transmission Line is one example which allows electricity to flow freely between Georgia and Turkey.

[17] K. Kaska and L. Trinberg, *op. cit.*, p. 11.

[18] *Ibidem.*

[19] These sectors were also assessed through the above mentioned study by Kaska, Trinberg, p. 16 and remarkably they showed the highest dependence degree on a scale between *"none to critical"*.

[20] For example the French television channel TV5 was the victim of a cyber-attack in April 2015, see '*TV5 Monde hack: "Jihadist" cyber attack on French TV station could have Russian link'*, 10th June 2015, http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html, accessed 27 January 2017.

the sectors were *not* dependent on *cross-border information infrastructure.*[21] The healthcare and water supply sectors were each estimated by only 18.18 per cent of respondents to be dependent of cross-border information infrastructure. In the traffic and transportation, public security and public order, nutrition/agriculture, and the media sector, 9.09% of participants assessed them as being non-dependent at all. Notable is that none of the sectors in this *"non-dependent category"* refer to the energy supply, ICT and telecommunications, finances, or government and administration sectors, meaning that all participants agreed that these sectors are very likely to show a cross-border dependency. This leads to the conclusion that these latter sectors are those in which a state should take a keen interest in comparing the operator's duties of the state in which the information infrastructure might be located, with its own regulatory norms.[22] If the operator's obligations of the other state do not meet security expectations, the owner or operator of critical infrastructure which is dependent on the cross-border information infrastructure would be well advised to take additional measures to ensure the desired security standards, such as security agreements with the foreign CII operator.

Protecting vital systems oftentimes means interacting across borders, and *protecting critical systems* means protecting them from cyber-attack. Within the military, cyber has therefore also become an additional dimension alongside the land, sea, air and space domains. At the national level, governments are tackling this challenge by developing National Cyber Security Strategies (NCSS), most likely prompted by the 2007 *denial of service (DoS)* and *distributed denial of service (DDoS)* attacks in Estonia.[23] The Cyberspace Protection Policy of the Republic of Poland, for instance, officially recognized cyber-attacks against Information and Communication Technology (ICT) as a national security threat.[24] The 2008 French White Paper on Defense and National Security emphasizes cyber-attacks, considering them a reason to shift national security thinking.[25] However, very few NCSS have addressed the cross-border dependencies aspect yet. Among the analyzed documents, the Estonian Cyber Security Strategy is one example of a yet very rare national document which addresses the topic of cross-border dependencies.[26]

2.2. Tackling the cyber risk – operators are the key players

2.2.1. The operator's list of duties

So far, very limited information is available in the existing international literature regarding the role of the operators in protecting cross-border located CII. This is striking since operators are the main players when it comes to cross-border safety. Therefore, while states are responsible for homeland security, operators are the main actors when it comes to securing infrastructure, and so it is important to know the legal obligations on the CII operator before deciding to connect across a border, something which might have undesirable safety implications. Scrutinizing the operator's obligations imposed by other nations will shed more light on how states deal with the threats concerning their own CII. How and to what extent states oblige their operators to mitigate risks and prevent vulnerabilities depends on the level of security that the state wants. In general, the operator's responsibilities can be determined either by enacting new laws, amending existing laws, or having self-imposed rules of conduct.

Operator's responsibilities can be divided into two categories: obligations of general nature and those concerning more specific situations.

[21] Kaska, Trinberg, *op. cit.*, p. 17.

[22] Research could not reveal any publication on a comparative legal view.

[23] See also Czosseck, Ottis, Talihärm: Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, http://www.ccdcoe.org/articles/2011/Czosseck_Ottis_Taliharm_Estonia_ After_the_2007_Cyber_Attacks.PDF; accessed 22 February 2017; An overview of the Cyber Security Strategies of NATO nations and their partners can be viewed at https://ccdcoe.org/strategies-policies.html, accessed 30 January 2017.

[24] Cyberspace Protection Policy of the Republic of Poland, 2013, p.8, https://ccdcoe.org/strategies-policies.html, accessed 30 January 2017.

[25] The French White Paper on Defence and National Security, 2008, p. 48, ff., http://www.mocr.army.cz/images/Bilakniha/ZSD/French%20White%20Paper%20on%20Defence%20and%20N%20ational%20Security%202008.pdf accessed 30 July 2016.

[26] Estonian Cyber Security Strategy, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf, p.6, accessed 30 January 2017.

2.2.2. General obligations

General obligations can be summarized into the four following categories:

- Implementing security measures;
- Maintaining security documentation;
- Notifying and reporting obligations and
- Monitoring obligations.

Implementing security measures can be regarded as the most important task for an operator. This requires implementing both organizational and technical measures. Organizational measures can include producing a risk management plan, managing cyber security incidents, taking care of CII control and audit, as well as taking care of personnel security and ensuring that only the designated group of people can gain access to the *CII system*. Organizing training and raising awareness about security risks among employees is another measure, requiring an increasing amount of time and effort for correspondence and communication. Technical measures include, among many others implementing *counter malicious code protection* and *user identity verification tools*, and *using cryptographic devices* and *cyber security incident detection tools*.[27]

Implementing security measures can involve network providers contacting affected users of the incident and providing them with patch tools for disruptive behavior originating from a consumer's computer. The latter, though, is more a matter of good practice.

Maintaining security documentation serves the operator primarily to support his own risk mitigation and service continuity. It includes the documentation of his risk assessment, the risk mitigation plan, and measures taken so far. Secondly, it serves supervisory aspects. Maintaining security documentation further proves the fulfillment of the set of obligations the operator has to carry out. It allows the controlling authority to keep track of what the operator has done to ensure the functioning of the vital service.

Notifying and reporting obligations are general obligations of an informational nature. In some national security acts they already include the reporting of an incident to the national authority.[28] The notification of a security breach or loss of integrity which has had a *significant* impact on the operation of networks or services must, under the EU Electronic Communications Framework Directive,[29] be reported to the competent national regulatory authority for companies providing public communications networks or publicly available communications services, and therefore constitutes common practice among EU member states. The upcoming EU network and *information security directive (NIS)* will contain a reporting duty in case of significant incidents for operators of certain sectors such as for the financial services, transport, energy and health.[30] However, the aspect of notifying the consumer is not a requirement placed on the companies, but rather a matter of good practice.[31]

Reporting an event to the national authority is of the utmost importance, since by this knowledge about new methods of attack or critical incidents with cross-sectoral or even cross-border impact can be gained. Reporting also serves a short-term objective of providing situational awareness about significant incidents in national networks. Awareness of these incidents is they of bigger or smaller impact helps to promote the analysis of attacks, early recognition of a new threat, and

[27] More examples are listed in chapter II, §5 of the Czech Act on Cyber Security, https://www.govcert.cz/en/legislation/legislation/, accessed 28th January 2017.

[28] For example the Czech Act on Cyber Security, §8 I, https://www.govcert.cz/en/legislation/legislation/, the 2015 German IT Security Act also included this obligation in § 8b (4), https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile, accessed 28th January 2017. The EU Network and Information Security Directive (NIS) which still needs to be approved by the European Parliament contains this reporting duty as well, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/, accessed 30 January 2017.

[29] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), Article 13a, para. 3, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0021-20091219&from=EN, accessed 30 January 2017.

[30] The EU Network and Information Security Directive (NIS) recently got approval by the EU Council, approval by the European Parliament is expected in summer 2016 and will probably enter into force in August 2016, http://www.consilium.europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/, accessed 30 January 2017.

[31] Art. 13 a para. 3 of the Directive 2002/21/EC states that the national authority concerned may inform the public where it determines that disclosure of the breach is in the public interest.

the early development of preventive tools from which a wide circle of addressees could profit. Yet, it requires additional administrative work and organization.

The operator might feel tempted not to report any incident, in particular not when there was just a short interruption of the service and little damage which the operator was able to manage alone. Unless it is a significant incident, a notification has not been required by law yet.

Announcing to a national coordinating authority that someone has exploited vulnerability within their systems and managed to disrupt the service, thus affecting the functioning of the asset, might have an unexpected high-cost impact. It might lead to loss of customer trust or damage to business reputation. Therefore, one could argue that private operators do not necessarily want to reveal that they have been the target of a cyber-attack. Yet, confidentiality provisions like §10 of the Czech Cyber Security Act, ensuring the non-disclosure of cyber security incident data are not integrated in every Security Act.[32] Aside from trying to avoid the incident becoming public, an additional administrative burden might lead to a negative attitude towards this obligation. And if the operator is neither obliged by law to notify the national authority, nor is there an effective controlling system being capable of overseeing compliance, there might be another argument for some operators not to proceed this way.

Finally, *monitoring obligations* means that the operator has to monitor his own network activity and ensure that the list of mandatory activities is fulfilled. It goes without saying that monitoring obligations are expected to be followed anyway by an operator who operates in accordance with due diligence standards.

2.2.3. Specific obligations

Specific obligations may result from specific legal acts which are meant to regulate a specific sector. This could be a Telecommunications Act, like for example the German Telekommunikationsgesetz, and paragraph 109 subparagraphs IV of which obliges the operator of a public telecommunications network to nominate a Safety Officer and to produce a safety policy that includes a variety of specified information. Among this detailed information, specifications are required on the kinds of threats expected, and the technical measures being taken in order to prevent potential disturbances.[33, 34]

Many of the generic and specific duties are permanent security measures, meaning that they have to be taken care of constantly. A smaller number refer to graduated security measures which need to be taken according to the current threat challenge.

3. Different safety cultures cause different obligations cross-border

Besides an individual threat picture, each state has an individual safety culture determined by its individual focus on security when developing information systems and networks. Therefore states differ in the way they adopt innovations and show different styles of behavior when using and interconnecting information systems.[35] Thus the list of responsibilities for operators in one country might be more comprehensive or stricter than that in another.

There are no internationally binding rules for protecting CII. Initiating a worldwide common approach which seeks a common high security standard seems to be impossible, as countries with a lower security standard probably do not see

[32] Although most countries do not have a Cyber Security Act, and despite the fact that general confidentiality obligations may derive from other legal acts – e.g. § 102 of the Estonian Electronic Communications Act, 01 January 2005, clear provisions like §10 of the Czech Cyber Security Act, referring to the non-disclosure of the company's name having suffered an incident cannot be detected on a widespread basis among those countries which adopted such an Act.

[33] German Telecommunications Act, 'Telekommunikationsgesetz' (TKG), 22 June 2004, last amended 19 February 2016, http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html, accessed 05th March 2017.

[34] For example also the Belgian Act 'Loi relative à la sécurité et la protection des infrastructures critiques' from 1st July 2011 obliges in its section 3, Art. 13 the operator to elaborate a security plan and provides a list of requirements for its content, http://centredecrise.be/fr/legislation/loi-01072011-securite-et-protection-des-infrastructures-critiques, accessed 05th March 2017.

[35] See also OECD, 'Guidelines for the Security of Information and Systems and Networks', http://www.oecd.org/internet/ieconomy/15582260.pdf, p. 8, or EU Commission doc. on CIIP: COM(2009) 149 final, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF, both accessed 09th March 2017.

the necessity to burden their operators with more tasks if the threat picture for their country does not require it. EC Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructure (ECI) and the assessment of the need to improve their protection is an attempt to reach a common standard at least EU wide. It was meant in its first stage for the energy and transport sector, but the information and communication technology sectors were already identified as future priority sectors during the draft period.[36] The topic on cross-border located critical infrastructures is addressed in the Directive by an information obligation and engagement request,[37] meaning that each member state has to notify any other which may be affected by ECI. With regard to the operator's obligation, it details the content of the operator's security plans which should include, inter alia, the selection of counter-measures.[38]

Different national approaches to implementing the Directive can form an unclear picture, in particular because translations of the implementation acts into other than the national language are oftentimes not provided.[39] Sometimes an unknown number of generic and specific obligations have to be detected in a patchwork of regulatory regimes and legal elements because such schemes relate to the operator's obligations. Thus, operators have to face an increasing complicated regulatory environment. Unfortunately, a study on the global picture of the operator's obligations which would highlight the differences of certain countries unfortunately is also lacking.

3.1. Operators bear the costs for CII safety measures

The increase of the operator's obligations comes with an increase of the costs of security measures, and who should meet these costs might become more and more of an issue. So far it seems that operators are the ones bearing first and foremost the costs of the required implementation of security measures.[40] Estimating the costs in advance is a formidable task, and depends in particular on the unknown number of sophisticated attacks, whose impact also remains unknown.[41] According to the president of Germany's Federal Office for Information Security, eighty percent of the standard attacks against security systems could be warded off if today's available security technology was implemented.[42] When asked how much a small company of about fifty employees should spend annually on cyber security the president of an IT security company replied $57,600, breaking it down into, amongst other things, secure email hosting for each employee, an antivirus service, and online backups.[43] A 2016 Ponemon Institute study involving 630 IT security practitioners revealed that the costs of malware containment for organizations to prevent malware-driven threats from stealing data and disrupting their systems amounts to an average of $1.3 million annually.[44] The legislative history of the new German IT Act reveals that the costs which each of the estimated 2,000 operators has to bear for reporting one single incident could add up to €660, estimating that the average number

[36] The Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final (the 'NIS-Directive') is currently at this point of research in its final steps: http://eur- lex.europa.eu/procedure/ENG/2013_27, accessed 09 March 2017.

[37] EU Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures (ECI) and the assessment of the need to improve their protection, 08th December 2008, http://eur- lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF, Articles 3-4, accessed 09th March 2017.

[38] *Ibidem,* see Article 5 and Annex II.

[39] See list of implementation http://eur-lex.europa.eu/search.html?qid=1429180435917&or0=DN%3D72008L0114*,DN-old%3D72008L0114*&type=advanced&SUBDOM_INIT=MNE&DTS_SUBDOM=MNE&page=1, accessed 09th March 2017.

[40] See also N. A. Sales, *Regulating Cyber Security, Northwestern University Law Review*, vol. 107 no. 4, 2013, p. 1506.

[41] See for more information on the economic cost of cybersecurity: T. A. Johnson in T. A. Johnson, *Cybersecurity Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, CRC Press, 2015, p. 255 ff. http://www.faz.net/aktuell/politik/inland/regierung-will-it-sicherheit-mit-gesetzentwurf-verbessern-13326788. html accessed 09th March 2017.

[42] http://www.faz.net/aktuell/politik/inland/regierung-will-it-sicherheit-mit-gesetzentwurf-verbessern- 13326788. html, accessed 09th March 2017.

[43] P. Clark, '*The Bill for Cybersecurity'*, http://www.bloomberg.com/bw/articles/2014-10-31/cybersecurity-how-much-should-it-cost-your-small-business, accessed 09th March 2017.

[44] Ponemon Institute, *'The cost of malware containment'*, http://www.ponemon.org/library/the-cost-of-malware-containment, p. 1, accessed 09 March 2017.

of significant incidents per year was up to seven.[45] Studies of the average annual cost of implementing security measures seem non-existent, and this has led to a call to national authorities to find out and clarify the financial impact for operators. Figures may vary from country to country, but investing in cyber security and providing personnel for the implementation of mandated measures seems to be one of the major expenses for the operators.

CONCLUSIONS

The conclusions are that designed by *cyber-power* refers to the exercise by a state which launches attacks on another state. Unit for cyber power, it seems, in this case study, the credibility of the threat coming from a state to engage in cyber-attacks. The more close to certainty, the better shape seems to be the nature of cyber power. Sufficiently diffuse this reason deprives the reader of Corel certainty commitment and ability to lead him in the end with a considerable impact. The mere intention or threats operationalization of employment in attacks shows itself not a risk factor, but rather a measure on a scale of (i) morality. The power is in this sense a deficiency that want highlighted.

Cyber-power in NATO methodology is used exclusively outside the theater of war. Total employment in the event of conflict kinetic is a truism. If military engagement, cyberspace is a part of the theater of war, going alongside PsyOps and propaganda attribution secondary units, with support functions. Cyber power and associated components, cyber war and cyber espionage, shall be exclusively periods of disengagement military: in times of peace. Army makes so even at the level of discourse, to ensure a permanent state of war, at least its cadres. Securitization issues by NATO perspective become corrosive when applied civilian models for periods of non-military employment. If contexts of military engagement, security of communication networks is one of the last components of the risk being assaulted fellow perpetrator or agent. Intervention components kinetics communications networks are secure. During periods of non-employment are components subject to securitization.

Reasons for securitization is accelerated can only be speculated: budget increased substantially to meet employment in *cyber-space* assumed the plot revealed by the possibility to explore a new environment for the study of conflict, the gain political capital from private corporations interested control the business model in which it performs or civil society component charmed by the idea of absolute order to enrich the vocabulary of political rhetoric and speculation politicking.

We can say that this terminology cyber power includes another term joint military thinking: *cyber-weapons*. It's really just a reconception term exploit, or tactics to exploit a vulnerability, which can be defined as constructs software that addresses one or more defects (vulnerabilities) in order to induce executable effect chosen by the attacker the limits imposed by the context of vulnerability presented in this article.

BIBLIOGRAPHY

1. NATO Parliamentary Assembly, *The Protection of Critical Infrastructures*, doc. no. 162 CDS 07 E REV 1, para. 72, http:/www.nato-pa.int/default.asp?SHORTCUT=1165, accessed 25 March 2017.

2. Estonian Cyber Security Strategy, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014- 2017_public_version.pdf, p.6, accessed 30 January 2017.

3. Cyberspace Protection Policy of the Republic of Poland, 2013, p.8, https://ccdcoe.org/strategies-policies.html, accessed 30 January 2017.

4. German Telecommunications Act, 'Telekommunikationsgesetz' (TKG), 22 June 2004, last amended 19 February 2016, http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html, accessed 05th March 2017.

5. The EU Network and Information Security Directive (NIS) recently got approval by the EU Council, approval by the European Parliament is expected in summer 2016 and will probably enter into force in August 2016, http://www.consilium.

[45] Reasoning of the draft of the new German IT Security Act, Drs. 18/4096 from 25th February 2017, http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf, p.5, the Act itself (German only) is available at: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1456916731 187, both accessed 09 March 2017.

europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurity-rule-adopted/, accessed 30 January 2017.

6. Kaska K. and L. Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, NATO CCD COE, Tallinn 2016, p. 10f., available at https://ccdcoe.org/multimedia/regulating-cross-border- dependencies-critical-information-infrastructure.html, accessed 25 March 2017.

7. Clark P., '*The Bill for Cybersecurity'*, http://www.bloomberg.com/bw/articles/2014-10-31/cybersecurity-how- much-should-it-cost-your-small-business, accessed 09th March 2017.