THIS PAPER HAS BEEN PUBLISHED IN Milan Sopóci (szerk.)

MANAŽMENT, TEÓRIA, VÝUČBA A PRAX 2013: ZBORNÍK Z PRÍSPEVKOV Z MEDZINÁRODNEJ VEDECKO-ODBORNEJ KONFERENCIE : 25. - 27. SEPTEMBRA 2013, LIPTOVSKÝ MIKULÁŠ.

398 p.

Konferencia helye, ideje: Liptovsky Mikulas, Szlovákia, 2013.09.25-2013.09.27. Liptovsky Mikulas: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2013. pp. 32-39.

(ISBN:978-80-8040-477-2)

THE ROLE OF THE CYBERSECURITY IN THE ECONOMY[1]

Péter Bányász

(Péter Bányász, PhD Student at National Univerity of Public Service, Address: H-1101 Budapest, X. Hungária krt. 9-11., Phone: +36 (1) 392-3500 29/457, Fax: +36 (1) 392-3502, 19-400, banyasz.peter@uni-nke.hu)

Abstract: Changes in the information technology have generated new challenges in the security of nations. In the history of warfare, in most of the times, there was an inequality between the fighting parties. The source of this inequality could have been economical, technological reasons or just the size of the parties. The modern warfare is shifting its focus to the information operations, in which area the parties are using the same weapons: computers. In these days, computers in network, the cyberspace is a stage of a constant fight. The international law is in the process of working out the legal environment for this fight. The stake is incredibly high; the fight is not only about gathering or defending classified information, but defending the critical infrastructures, institutions responsible for the safety of homeland security and economics. The presentations today are going to put defending our critical infrastructures in perspective of the role of the cyber security and its effect on economic security.

Keywords*: cyber security, critical infrastructure protection, defense economics, information warfare, cyber war*

INTRODUCTORY THOUGHTS

In our century, a sort of paradigm change is observed in the field of information warfare. Changes in the information technology have generated new challenges in the security of nations. The significance of information warfare is best proved by the Esthonian-Russian cyber war taking place in 2007 or the use of Stuxnet virus for paradigm change against particle acceleration of Natanz putting back Iran's uranium enrichment efforts with two years. By using only computer systems the attackers may bomb the attacked country back into the "digital stone age" without any conventional warfare (Bányász-Orbók 2012).

[1] This artice was elaborated with the support of the Critical Infrastructure Research Project TÁMOP-4.2.1.B-11/2/KMR/001

In the cyberspace, a continuous war is taking place with the intention not only to obtain the most possible state or industrial secrets but also to probe the vulnerability and weaknesses of the enemy that could be effectively used to weaken or even fully destroy the enemy in the case of a potential conflict.

There is no day without learning about a cyber attack against a state or market operator. During the research work made for this article, one of the most significant pieces of news was about an attack against a critical infrastructure of the United States of America where only the response to it was perhaps even more frightening: the intrusion against the U.S. Army Corps of Engineers[2] . The attackers – supposedly Chinese hackers – obtain information on 79 thousand dams. Dams are not only major elements of energy production but may even threaten the lives of people by flooding areas if control over them is obtained. This is even worsened by the response of USACE to the happenings: they notified the persons concerned of the intrusion in e-mails and sent the new ID and password (Gertz 2013) in an attached file to create the new security protocol.

THE CONCEPT OF ECONOMIC SECURITY

During the period of the bipolar world order, security was basically the primacy of military security, however, by now the concept has changed and requires a complex interpretation[3]. An important, or perhaps the most important element of this interpretation is economic security[4]. We cannot speak of security or economic security if its concept is not interpreted in a complex way. The appearance of economic security in national and international relations must be distinguished. In the first approach, economic security is the ability of the state to maintain and continue the nation's existence despite all external threats and pressures in addition to keeping the state's sovereignty and independence. In our globalised world, maintenance of this is an extremely complex activity since various state and non-state operators are superimposed on each other and consequently depend on each other to such an extent that the termination or reduction of this interdependence is almost impossible[5]. This trend will be even more relevant as a result of the intensification of interdependence in the world economy in the future.

Vulnerability to the increased external dependence and external impacts will further complicate the determination of the actual content of economic security. Though integration offers the possibility of the increase of economic efficiency the interdependence and the appearance of factors threatening the economic security of certain national economies are unavoidable. As the global financial crisis in 2007 proved, that kind of superimposition of the economies will collapse the economies of other nations in a domino effect.

In our article we intend to present neuralgic points (legal environment, protection of critical infrastructures and cyber attacks against them) that are relevant in the study of correlations between cyber security and economic security.

---

[2] USACE is a federal agency responsible for the conditions and construction of dams, canals and flood protection.

[3] During the cold war, the direction of threat was rather predictable, but in the new security environment new challenges have strengthened, including terrorism, organised crime, weapons of mass destruction, climate change etc.

[4] These include, among others, political, social and environmental dimensions.

[5] Perhaps this difficulty is best illustrated by the dependence of Ukraine on the Russian gas which offers the possibility to Moscow to influence political decision-making via the Gasprom.

THE CYBER WAR AND THE LAW

The attacks are multilayer ones: they target the suppliers[6], employees in administration[7], critical infrastructures[8]. The purpose of our study is to increase scientific discussion on the topic and to emphasise the importance of strengthening cyber protection abilities[9].

Though threats from the cyberspace are real risks there are still often deficiencies found in the cyber protection capabilities of certain states. Even in Hungary, several authors call the attention to the risks present in this field. These include study *"Digitális Mohács- egy kibertechnikai forgatókönyv Magyarország ellen" (Digital Mohács and a Cyber Technical Scenario against Hungary)* by László Kovács and Csaba Krasznay in which the authors used only open-source intelligence to evolve how attackers could immobilise Hungarian critical infrastructures in a well-organised information operation (Kovács-Krasznay 2010). However, to be able to use proper responses to the arising threats the decision-makers must know the risks and this is why awareness of the importance of the complex interpretation of critical infrastructures is required (Horváth 2010).

On 19 July 2012, Barack Obama, President of the United States of America submitted the Cybersecurity Bill to the Senate which started giving the highest priority to the long debated issue of the demand on proper response to cyber attacks increasing at an incredible rate[10]. Pentagon has been working on rules planned to be published by the autumn of 2013 and to be introduced in the next year that will provide security standards for privately owned public utilities and other public utilities of vital importance but supported by the Army. The Department of Defence has been urging legislation for a long time as a guide must be worked out for the government and business operators to reduce cyberspace threats. Though many are averse to the possibility of ruling from a central computer more and more owners of critical infrastructures have asked the Government to work out uniform rules (Sternstein 2013). Considering that on the basis of the report made by the Department of Homeland Security of the United States 198 attacks were made against industrial control systems in 2012 efforts made to establish a stringent regulation are more than reasonable (Wire 2013). At this point we must note that in response to the rapidly increasing number of attacks a market based on the security demands of certain industries has been gradually growing, and for example in the oil and gas industry specialised companies achieved incomes amounting to 18.31 billion dollars which amount is expected to increase to 31.37 billion dollars by 2021 (Net Security 2013).

But not only did the U.S. recognise the risks. Troels Oerting Assistant Director of Europol has pointed out that the European governments must be ready to manage attacks causing damages of several billions of Euros (The Information Daily 2012). Symantec has been yearly studying the current trends of cybercrime to give an overall picture of the effects of cybercrime on consumers and of the security consequences of the development and application of new technologies. The result of the survey for 2012 is alarming: cybercrime has 18 victims per second, i.e. one and half million victims at

[6] See The Lockheed or the QinetiQ North America.

[7] See Red October malware.

[8] Among them, energy grids are the major targets since all other services depend on them: “if there is electricity then everything is available” (Net Security 2012).

[9] We must admit that the attackers will always have an advantage against the protectors and if we do not improve our attacking capabilities we will lag behind for ever. For details on the topic see “A kibertér konfliktusok változásai” (Changes of the Cyberspace Conflicts) by Gábor Berki (Berki 2013).

[10] The number of attacks increased by 400% in 2012 as compared to 2011 (Info Security 2012).

international level. Breaking down the financial loss to individual level the average damage caused to a user is ca. 197 dollars (Symantec 2012).

In February 2013, the European Commission published its cyber security strategy *"EU Cyber security plan to protect open internet and online freedom and opportunity"* specifying five priorities:

- *Achieving cyber resilience*
- *Drastically reducing cybercrime*
- *Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)*
- *Developing the industrial and technological resources for cyber-security*
- *Establishing a coherent international cyberspace policy for the European Union and promoting core EU values"* (EC Communication 2013).

The communication gives a list of several statistical figures to emphasise the importance of the establishment of common cyber defence capabilities since attacks are severe security and economic challenges and only common actions can properly manage them. According to experts, there is a 10% chance of the collapse of the critical infrastructure in this decade that may cause economic damages amounting to 250 billion dollars. Fortunately, Hungary does not lag behind and was one of the first countries to establish a uniform legal background for threats from the cyberspace with the adoption of bill on "the electronic information security of state and local government bodies" by the Parliament in April 2013. The law provides for the setting up of a governmental body reacting rapidly, for the survey of critical infrastructures and according to the law a military cyber defence task force (to be newly established) will be also involved in the protection (Act L of 2013).

We should not study the subjects of legislation only by establishing norms for the protection of infrastructures of vital importance. The Russian-Estonian cyber war of 2007 has called the attention to the deficiencies in regulations on cyber attacks in the international law. In the cyber war, a NATO member state was attached which is interpreted as an attack against NATO itself on the basis of the principle of collective defence in accordance with Article 5 of the alliance. So NATO interpreted the happenings as a non-military attack, not accidentally. Today more and more people state that cyber attacks are acts of war and based on this they have a right to self-defence. One of them is Harold Koh Legal Adviser of the U.S. Department of State (Nakashima 2012) or Tony Blair's former National Security Advisor, Sir Richard Mottram (Wheeler 2011), and the so-called Tallinn Manual 2013 has been drawn by international experts at the request of NATO to serve as a recommendation as to the international legal principles based on which cyber warfare should be regulated. The manual tries to interpret the online war on the basis of the principles of classical warfare, following the Geneva and Hague conventions, and is declared to protect civilians. Consequently, it prohibits attacks against hospitals, water and nuclear power-plants. Attacks causing death or particularly great damages are considered acts of war which serve as a basis for exercising the right of response with conventional means, and hackers making the attack are interpreted not as civilians but as soldiers. However, it is important to note that it is extremely difficult to prove who the attackers were. As the above Russian-Estonian cyber war or the case of Stuxnet has also shown that despite the fact that the attackers were known no definite evidences were available to confirm the Russian or the American-Israeli involvement. But based on the specification of cases considered acts of war in the Tallinn Manual the right of self-defence may be exercised in both cases (particularly if there is an attack resulting in great damages or made against a nuclear power-plant).

In the summer of 2012, the U.S. and China started bilateral negotiations intended to restrict online attacks, implement better communications and reduce third party related risks (Lemos 2012). But we should not have an illusion; there is a large-scale cyber war between these two countries behind the scenes. Let's consider the study of Mandiant Security Company according to which several hundreds

of terabytes of information were obtained by hackers in attacks sponsored by the Chinese Army (Mandiant 2013). In May 2013, the two states sent messages to each other via the media and accused each other of series of attacks, posing as victims (Global Times 2013). In Pentagon's yearly report studying the Chinese military potential, China is clearly made responsible for the cyber attacks on the United States (Dod Report 2013). Nevertheless, in America more and more people think that the attacks destroy the creditability of the country, while foreign investors fear that intellectual properties owned by them would be acquired by hackers (Jones 2013). In response to the report of the Department of Defence, democratic Carl Levin and Jay Rockefeller and senators republican John McCain and Tom Coburn introduced the *"Deter Cyber Theft Act"* intended to combat data thefts in a more stringent way by providing protection for businesses and their confidential data against foreign hackers and governments (Kerr 2013).

CONCLUSION

The principle of *"the best defence is a good offence"* is assigned to Napoleon, and naturally this can apply also to cyber attacks. More and more states recognise the necessity of this and establish their own military units specialised in cyber attacks similarly to China[11]. Fearing that their critical infrastructure would be attacked, India authorised the Defence Intelligence Agency and the National Technical Research Organisation to carry out not detailed attack operations if necessary (Muncaster 2012). The Pentagon's Cyber Command targets to set up 13 offensive teams by 2015 (Nakashima 2013). The new teams will be established as part of extensive governmental efforts to protect the country against attacks that may affect for example the Wall Street or the electric grid. Naturally, Russia does not lag behind (as it has been indicated also by the DOS attacks against Estonia or the attacks made in the Russian-Georgian War one year later as a supplementation to the conventional war), but Iran is also of importance with its army of an estimated number of 4 to 5 thousand hackers which is presumably the 4th greatest unit of that nature[12] (Iran invested one billion dollars in its establishment which is reasonable after the destruction by Stuxnet). The cyber army of 3000 heads of North Korea is not negligible either, which can increase the risk if it is owned by a regime ready to make unpredictable and irrational decisions (Ponemon 2012).

In this article, we tried to present the effect of cyber attacks on the economy. We hope that we have been able to confirm that cyber threats from the dramatically increasing number of attacks against critical infrastructures significantly affect the economy of states. The risk is increased by the fact that it is easier to attack critical infrastructures than to protect them. The costs of protection are high[13], however, the legislators may not give proper priority to it due to budgetary restrictions. If we consider that the organisations under examination were exposed to some kind of cyber attack every three minute in 2012 (FireEye 2012) and that 94% of the attacked companies do not know that their systems

[11] In the above cited Mandiant report, unit 61398 belonging to the People Liberation Army was designated as the perpetrator of the attacks from China.

[12] The attack against the Saudi Aramco deleting everything on ca. 30 thousand computers and the online invasion against American banks are attributed to them.

[13] In a study, the costs attributed to cyber attacks increased by 5% from annual costs of 8.4 million dollars in 2011 to 8.9 million per company (Hanula 2013), but China will spend enormous costs on its strengthening in the next years due to their fears about the security of the electric grid, and therefore the Chinese cybersecurity market will develop at an immense rate. It will increase from 1.8 milliard dollars in 2011 to 50 milliard by 2020, which is an annual expansion by 44.7%, while Europe and North America will spend only 16 billion for this purpose in the same period (Dark Reading 2012)

have been hacked (Pitchford 2012), the threat is further increasing. In our opinion, four major areas must be developed to be able to create successful cyber defence capabilities:

- legislation,
- proper budget,
- expansion of education,
- close cooperation with research workshops.

The question is rhetorical: are we ready?

REFERENCES

2013. Act L of 2013: *On the electronic information security of state and local government bodies. Hungarian Official Journal No 69*, 25 April 2013, ISSN 2063-0379.

AGENCIES: Chinese media lambaste US hacking allegations, In. Global Times, 24 February 2013, ISSN: 2095-2678 (English Edition), http://www.globaltimes.cn/content/763654.shtml (4 August 2013).

Press release of the EUROPEAN COMMISSION: *EU Cybersecurity plan to protect open internet and online freedom and opportunity*, 7 February 2013., http://europa.eu/rapid/press-release_IP-13-94_hu.htm (4 August 2013).

THE NORTH ATLANTIC TREATY 4 April 1949 http://www.nato.int/cps/en/natolive/official_texts_17120.htm .

BÁNYÁSZ, Péter- ORBÓK, Ákos: *A NATO kibervédelmi politikája és a kritikus infrastruktúra védelme a közösségi média tükrében*. Hadtudomány Online, 2013., ISSN: 1215-4121, http://www.mhtt.eu/hadtudomany/2013_e_Banyasz_Peter_Orbok_Akos.pdf (4 August 2013).

BERKI, Gábor: *A kibertéri konfliktusok változásai*, In. Hadmérnök, 2013., VIII. évfolyam 1. szám, http://www.hadmernok.hu/2013_1_berkig.pdf (6 August 2013).

DEPARTAMENT OF DEFENSE: *Annual Report to Congress- Military and Security Developments Involving the People's Republic of China 2013*, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf (2 August 2013).

FireEye Inc.: *Advanced Threat Report – 2H 2012.* , 2013., http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-threat-report-2h2012.pdf (2 August 2013).

GERTZ, Bill: *The Cyber-Dam Breaks, In. The Washington Free Beacon*, 1 May 2013 http://freebeacon.com/the-cyber-dam-breaks/ (2 August 2013).

HANULA, Zsolt: *A neten már zajlik a harmadik világháború*, In. Index, 2013. május 6., ISSN: 1585-3241, http://index.hu/tech/2013/05/06/a_neten_mar_zajlik_a_harmadik_vilaghaboru/ (6 August 2013).

HORVÁTH, Attila: *Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének szükségességét és védelmének fontosságát*, Hadmérnök, 2010., V. évfolyam 1. szám, ISSN 1788-1919, http://hhk.uni-nke.hu/downloads/tudomanyos_elet/EU_palyazatok/2012/horvathattila.pdf (1 August 2013).

JONES, Terril Yue: *Cyber attacks hurt China's credibility: U.S. official*, In. Reuters, 9 April 2013, http://www.reuters.com/article/2013/04/09/net-us-china-usa-cyber-idUSBRE93806620130409 (2 August 2013).

KERR, Dara: *Senators propose law to go after foreign cybercriminals*, In. CNet, 7 May 2013 http://news.cnet.com/8301-1009_3-57583379-83/senators-propose-law-to-go-after-foreign-cybercriminals/ (1 August 2013)

KOVÁCS, László- KRASZNAY, Csaba 2010: *Digitális Mohács- Egy kibertámadási forgatókönyv Magyarország ellen*, Nemzet és Biztonság III. szám, pp. 44-56, ISSN 1789-5286.

LEMOS, Robert: *U.S., China Talks Address Cyber-Weapons, Not Cyber-Spying*, In. eWeek, 18 August 2012, ISSN: 1530-6283 http://www.eweek.com/c/a/Security/US-China-Talks-Address-CyberWeapons-not-CyberSpying-329861/ (4 August 2013).

MANDIANT: *APT1- Exposing One of China's Cyber Espionage Units*, 2013., http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (7 August 2013).

MUNCASTER, Phil*: India to greenlight state-sponsored cyber attacks*, In. The Register, 11 June 2012, http://www.theregister.co.uk/2012/06/11/india_state_sponsored_attacks/?goback=.gde_3502864_member_123369450 (1 August 2013)

NAKASHIMA, Ellen: *Pentagon creating teams to launch cyberattacks as threat grows*, In. The Washington Post- National Security, 12 March 2013, ISSN: 0190-8286, http://www.washingtonpost.com/world/national-security/pentagon-creating-teams-to-launch-cyberattacks-as-threat-grows/2013/03/12/35aa94da-8b3c-11e2-9838-d62f083ba93f_story.html (1 August 2013)

NAKASHIMA, Ellen: *U.S. official says cyberattacks can trigger self-defense rule*, In. The Washington Post- National Security, 19 September 2012, ISSN: 0190-8286, http://www.washingtonpost.com/world/national-security/us-official-says-cyberattacks-can-trigger-self-defense-rule/2012/09/18/c2246c1a-0202-11e2-b260-32f4a8db9b7e_story.html (2 August 2013)

NATO Cooperative Cyber Defence Centre of Excellence 2013: *Tallinn Manual on The International Law Applicable to Cyberwarfare*, Cambridge University Press, http://issuu.com/nato_ccd_coe/docs/tallinnmanual?mode=embed&layout=http%3A%2F%2Fskin.issuu.com%2Fv%2Flight%2Flayout.xml&showFlipBtn=true

PITCHFORD, Matt: *Former FBI cyber expert: 94% of cyber security breaches unreported*, In. The Daily Caller, 18 June 2012, http://dailycaller.com/2012/06/18/former-fbi-cyber-expert-94-of-cyber-security-breaches-unreported/ (9 August 2013).

PONEMON INSTITUTE: *2012 Cost of Cyber Crime Study: United States*. http://static.knowledgevision.com/account/idgenterprise/assets/attachment/HPESP_WP_PonemonCostofCyberCrimeStudy2012_US.pdf (2 August 2013).

STAFF WRITER: *China's Cyberattack Fears To Spark Massive Defense Spending*, In. Dark Reading, 13 September 2012, http://www.darkreading.com/vulnerability/chinas-cyberattack-fears-to-spark-massiv/240007265 (9 May 2013).

STAFF WRITER: *Cyberattacks up 400% since 2011*, In. Info Security, 2012. augusztus 30., ISSN: 1754-4548, http://www.infosecurity-magazine.com/view/27876/cyberattacks-up-400-since-2011/ (7 August 2013).

STAFF WRITER: *Energy grids are prime attack targets*, In. Net Security, 18 July 2012, http://www.net-security.org/secworld.php?id=13266 (5 August 2013).

STAFF WRITER: DHS: *Industrial control systems subject to 200 attacks in 2012*, In. Homeland Security News Wire, 14 January 2013 http://www.homelandsecuritynewswire.com/dr20130114-dhs-industrial-control-systems-subject-to-200-attacks-in-2012 (6 May 2013).

STAFF WRITER: *The EU points its guns at cyber criminals*, In. The Information Daily, 9 August 2012, http://www.egovmonitor.com/node/53238 (4 August 2013).

STAFF WRITER: *Vulnerability of oil and gas infrastructure drives security investments*, In. Net Security, 15 January 2013, http://www.net-security.org/secworld.php?id=14238 (5 August 2013).

STERNSTEIN, Ailya: *Pentagon will require security standards for critical infrastructure networks*, In. Nextgov, 15 February 2013, http://www.nextgov.com/cybersecurity/2013/02/pentagon-will-require-security-standards-critical-infrastructure-networks/61328/ (7 August 2013).

Symantec: *Norton Cybercrime Report-2012*, http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf .

WHEELER, Brian: *Cyber attacks 'acts of war' - Sir Richard Mottram*, In. BBC News, 16 February 2011, http://www.bbc.co.uk/news/uk-politics-12485147 (3 August 2013).