CENAA
Centrum pre európske a severoatlantické vzťahy

Policy Papers

CYBER WAR OF THE STATES: STUXNET AND FLAME VIRUS OPENS NEW ERA OF WAR

Veronika Macková

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. One of the most problematic elements of cyber security is the quickly and constantly evolving nature of security risks (Rouse, 2010).

The purpose of this paper is to provide a realistic assessment of the capabilities, means, purposes of selected country, to conduct and show that cyber security of the state is a focal issue of present defence politics. On top of this will prove that the viruses (Stuxnet and Flame) have opened a new era of cyber war and cyber security.

Computer-to-computer attack against the state or against regional adversaries. This paper takes that there is no such thing as “perfect” IT security. It is proven, that cyber security of Iran is a focal point of cyber war, especially when we are talking about nuclear weapons. This report is focused on one state only-Iran and the problematic of nuclear weapons regarding to computers and their security. The different sections of the essay focus on a various issues, viruses and problematic of the cyber security of the country. For example, hackers seem always able to keep one step ahead of latest software security program, for which states pay billions of dollars. As for instance, some secure portions of the US defence computer systems are connected to the

public network. As Adam Vincent said: “The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly...”

The Weak State Security?

Without no surprise that recent events of the various hacks, cracks, online intrusions and black-out of the states' security systems which have been dominating headlines of the newspapers and news, there's been a loud, cry and scream from companies and governments for increased investment in something called “cyber security”. It's a term that has in some way is seen as a “cure” for a security of the states. Unfortunately this “cure” doesn't work so often, as is proved by recent events. So why is the computer-security so important? Cyber security helps us to prevent and detect unauthorized use of a computer or the whole operation system (OS). Prevention measures help to stop unauthorized users (known as “intruders”) from accessing any part of OS. Different detections determine whether or not someone attempted to break into a system, whether the intruder was successful or not and what he may have done or will do.

Our daily life, economic and national security depends on safe, stable and resistant cyberspace. “Deloitte & Touche's 2003 Global Security Survey, examining 80 Fortune 500 financial companies, finds that 90% of security breaches originate from outside the company, rather than from rogue employees. ‘For as many years as I can remember, internal attacks have always been higher than external,’ said Simon Owen, Deloitte & Touche partner responsible for technology risk in financial services. ‘60 to 70 per cent used to be internally sourced. But most attacks are now coming from external forces and that's a marked change’” (Nash, 2003).

Unfortunately, intruders are always discovering new vulnerabilities, “holes”, to exploit in computer system. Why did the threat change in such a short period of time? Sadly we have no definite answers. But there are a few possible answers to this question. “First the emergence of automated worm attacks starting with Code Red1 in July 19, 2001 have meant that many of the intrusions have become non-directed and automated. The control system has become just a target of opportunity rather than a target of choice” (Alvi, 2004). Then we have common OS-as Windows, Linux or Mac and of course various system applications, which dominate on the trade. These programs are vulnerable and easy to attack by viruses and hackers. On top of this we have an increasing interconnection of critical systems, for example SCADA (The Electronic Attack Threat to Supervisory Control and Data Acquisition) network-which still believes to be a “secure” system. To deal with the current problematic, different organizations are promoting different adaptive approaches. For instance the National Institute of Standards and Technology (NIST) recently updated guidelines for monitoring and preventing the computer software. According to the analysis of 2010, US allotted over $13 billion annually to cyber security.

Cyber security, cyber warfare and of course cyber war are topics which have been much-more discussed daily. Recent attacks on corporate or government systems have brought the issue on surface. As a reaction to this, many of the states did not use the chance to discuss and sort out this problematic. They closed their “doors” and made the cyber security issues as a taboo and started to pretend, that no such as cyber-attacks exist.

"The Cyber War is more complex. Some tend to perceive it as more separated from traditional warfare. Pioneers of net-war, John Arquilla and David Ronfeldt define it as —net-war refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an inter-netted manner, often without a precise central command" (Aequilla, Rondfielt, 2001:6).

Iran and Beginning of War

Iran's nuclear program is one of the most problematic issues. To consider being one of the world's most volatile regions with "unbreakable" defence program which American and European officials believe is threat for the whole world. Iran's officials say that their goal is to generate electricity without dipping into the oil supply through nuclear weapons. Iran and West countries have been negotiating over the nuclear program for decades. However since 2011 the situation has changed. The position of West and Iran (against Iran's defence and oil politics) has sharpened. And thanks to economic crisis and the way how countries negotiate, will sharpen even more.

In late summer of 2012, international nuclear inspectors reported that the process of building a deep-underground site of nuclear fuel has progressed. "Mr Netanyahu warned that Iran's capability to enrich uranium must be stopped before the spring or early summer of 2013." (Gladstone and Sanger, 2012) "The report also showed that Iran's stockpile of its most sensitive nuclear material—which could relatively quickly be processed further to bomb-grade uranium—had grown and was getting closer to an amount that could be sufficient for a nuclear weapon. The report also said that satellite photographs show Iran has worked for months to alter another site that the agency has long suspected may have been used for weapons-related experiments." (Dahl, 2012)

What would happen if you unlock a door at the top Iran's nuclear laboratory? How about one stolen computer with data marked as top secret? Would be the computer stolen to be resold for a hacking, or for weapons of mass destruction? Or just for fun, to prove to the world that none of the countries are safe. The reason of this "attack" we may never know. The information can be sold for billions or can get just disappeared... Or we may find out the hard way-the way which could destroy most of the countries.[1] Situations like this are common in every industry which works with sensitive information. But the whole world wishes, that this data would not be used from a nuclear weapon facility. Everyone knows, there is no such thing as 100% security- especially the cyber security of state regarding nuclear weapons. Security is an on-going and unfortunately never ending, vigilant process. The militarization of cyberspace has been under way for more than 16 years. However only in the last couple of years have the signs appeared that the United States are changing their cyber security. The main reason was the attacks from September 2001 and the on-going negotiations with Iran- as one of the non-controlled country in nuclear weapons problematic. It is scandalous to believe that such as computer worms, viruses are possible to start nuclear war? Recent cyber-attack- as Stuxnet and Flame- have not only made a "mess" in politics and diplomacy but brought on

[1] As for instance Estonia in 2007

a table questions such as: Could cyber warfare start nuclear warfare? Did these viruses open a new era of war? How long the states can keep up with the lies, that the security of state and nuclear programs, researches are secure?

The New Era of War

This brings us to the main topic of this paper. In the following section, different examples prove, that the cyber security of Iran and viruses which were used against Iran have opened a new era of war between states. The Internet has experienced a breath-taking expansion over the past two decades. From a tiny network, this was limited for science purpose only to a worldwide network which counts more than three billion of users. Everyone who knows basic things in computing knows that every computer which is connected to the Internet is breakable. Different applications for the Internet include the rise of a cyber-economy- this includes financial and banking transactions, key control systems, sharing and storing different, even top- secret information... In addition to the social benefits, the cyber world has proven to be no stranger to attacks, conflicts and crimes. Many scientists see the cyber war even more dangerous than the era of the Cold War. And we are finally starting to understand their concerns. Critical infrastructure is growing progressively more vulnerable to cyber-attack. Senior leaders around the world have expressed concern that the risk of cyber war is growing every day. For most of them the potential danger form computers is seen as the catastrophe of Pearl Harbour. As we could see in 2007 in Estonia, when the whole system went down, because the state was "over- connected" with the Internet. But are such concerns valid? While it is difficult to undertake an assessment of a form of warfare about which relatively little is known? The cyber security is a theme about which states do not like to talk. Is the reason to believe that the potential attack on relatively prompt, catastrophic levels? Cyber weapons appear to be capable of meeting the minimum definition of catastrophic destruction in that they could wreak "extreme misfortune" on Israel. For instance, disturbing critical infrastructure for some time. The costs of such an attack would weak the country in terms of some or all of the following:

• Accepting the economic losses;
• Adapting the infrastructure;
• Abandoning reliance (i.e., returning to the pre-Internet era, circa 1980).

Most countries and businesses are already accepting losses associated with cyber-attacks as a cost of doing business. On the one hand, most of them are working to adapt and upgrade their systems to minimize their vulnerability but on the other hand, we have states and companies, which are avoiding to change their way of protecting them against the attacks. Or even better, enterprises and governments who are trying to prove, that their security is unbreakable. And this is obviously not possible. Could cyber warfare nullify nuclear weapons in Iran? Is it really outrageous to believe that cyber weapons, for instance computer worms, viruses or malware, could have the capacity to cause nuclear war? In the quite recent actions of hackers, have not only proven the fear but also have "put couple of states on the knees". The recent cyber-attacks, including Flame and Stuxnet, have not only made governments aware that they have the security on the low level, but have invited a crucial question: Could cyber warfare supplant nuclear warfare? The cyber weapons have the possibility to start the nuclear war, delay it or just "blackmail" the states or

companies. As was already mentioned below, every computer connected to the Internet is susceptible to a computer virus. On top of this, computer can be comprised or attacked without being connected to the Internet. One of the examples was developed by the United States and Israel. The aim of the virus was the Natanz uranium enrichment facility in Iran. As known, the Natanz facilities were not connected to the Internet. However, someone had to upload the computer virus from the Iranian complex- simply used a memory stick- and then just infect the system. The result of this attack was to postpone and setback for several years.

Over the last couple of years, Iran has become one of the main target of a series of notable cyber-attacks, some of were linked to its nuclear programs and research. The most famous one is Stuxnet, a computer worm who postponed several nuclear programs for years. “According to an article in The New York Times in June 2012, during President Obama‘s first few months in office, he secretly ordered increasingly sophisticated attacks on Iran's computer systems at its nuclear enrichment facilities, significantly expanding America’s first sustained use of cyber weapons. After Stuxnet was detected around the world, temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium” (New York Times, 2012) At the beginning, Iran denied that their computers have been hit by Stuxnet. In 2011, Iran announced that the Iran's security started its own military cyber unit. The US administration later on informed the media that the Iran's nuclear program was set back up to two years. However many computer experts are sceptical. Some say that Iran's enrichment levels are so low, that it will take more than 2 years to get completely recovered, however others say, that Iran's nuclear research is so flexible, that they will recover in less than 15 months. And which possibility is more likely? Unfortunately we don't know. The Iran's research is in many ways so secure that scientists can only guess.

Stuxnet as the Main Threat

Stuxnet appears to be the first time known virus, used by the United States, to cripple another country's infrastructure. Used a computer code, what until then was possible only by bombing a state, or sending in agents or soldiers to plant the weapons. “The code itself is 50 times as big as the typical computer worm, Carey Nachenberg, a vice president of Symantec, one of many groups that have dissected the code, said at a symposium at Stanford University.”(New York Times, 2012) Stuxnet is one of the most sophisticated and intelligent computer worm. Discovered in the second half of 2010, easily spreads via Microsoft Windows and mainly focused on Siemens industrial software and its equipments. The worm's “attack” is in some way very easy. It spreads secretly, but consists of a high-specialized malware lay-load to hit only few-very important data in the system; for instance programs which are controlling and monitoring processes or even more, taking care of the cooperation with different systems and applications. So far as known, there were made 5 different variants of Stuxnet which targeted five Iranian organisations. As a result of these attacks, Iran nuclear program has been damaged by Stuxnet.

On 1st of June 2012, an article in The New York Times blamed that Stuxnet is part of a US and Israeli intelligence operation named “Operation Olympic Games” which started under former president George W. Bush and has expanded under current president Barack Obama. This message was later on confirmed by different newspapers or televisions. On top of this “chaos

and madness" about security of the states and companies, the United States confirmed that they have lost control of it. This message was seen by many scientists and hackers as an invitation card for cyberwar. "Obama ordered cyber-attacks on Iran's nuclear programme but created a super-virus that is now 'out of control'". (Conway, 2013) Yes, Barack Obama and the U.S. Government secretly have changed the war against Iran's nuclear programme, but created a virus that has escaped into the rest of the internet world. Thanks to this virus, the cyber-security of most of the states has been damaged. The United States have opened "a door" to the new era of war, attacks and suspicions.

The virus Stuxnet makes complex modifications to the system. It can change motors, pumps, conveyor belts. It can stop a factory and on top of this can easily cause things to explode, that includes bombs, warheads and nuclear weapons as well. Stuxnet is one of the most complex and unusually big viruses in the computer science. It uses a driver stolen from Realtek Semiconductor Corp and uses multiple vulnerabilities and drops to the system. Both Governments hoped to set back Iran's research programme and on top of this US hoped to keep Israel from possible military attack. According to the Ars Technica website, the Stuxnet code was supposed to work within Natanz- Iran's facility. A bit of code was at the beginning used for a map out the network connections within the Natanz and then reported back to the United States. During the presidency of George W. Bush, had the US a digital map of Natanz and its different control hard-wares, which helped the American scientists to start a testing to sabotage and slowly destroy Natanz. Unfortunately in 2010, Stuxnet escaped and did everything what it was designed to not to do- spread around the world. "'We think there was a modification done by the Israelis,' one of the briefers told the president, 'and we don't know if we were part of that activity.'" (Conway, 2013)

This brings us a question, how long are states capable to defence themselves? How are you able to chase someone if the person or a group does not need to be present during an attack? How you can chase something which you cannot even see? How to detect a hacker attack, if the Internet is seen as a labyrinth of different connections and possibilities? The Stuxnet virus, that sabotaged the Iranian nuclear program, could be easily used against the US infrastructure and security too. The full result of the damage to Iran's nuclear research and equipment by Stuxnet was, is and will be always a matter of speculation. The outside world has almost no access to information about Iran's nuclear program. Iran several times refused a co-operation with U.N. Security Council and substantiated with peaceful purposes. "Most computer vulnerabilities can be exploited in a variety of ways. Hacker's attack may use a single specific exploit, several exploits at the same time, a misconfiguration in one of the system components or even a back door from an earlier attack." (Kaspersky Lab ZAO, 2013) Because of this, detecting hacker attack is not easy task at all. And if we are talking about viruses, Stuxnet or Flame, which are operated by hackers, there will never be 100% guarantee of detecting a hacker. Was Stuxnet written by a government? Yes, it was. Will Stuxnet spread forever? The last version of Stuxnet had a "kill date" of 24th of June 2012, which means that this is the last date of spreading. However the person who made the Stuxnet knows how to change the code, and can easily make a new version- more sophisticated and even more dangerous.

On 9th of November 2012, RT newspaper published an article, where Chevron admitted that since 2010 are fighting with Stuxnet. Until now, Chevron managed to make fighting a well-

kept secret. “We’re finding it in our systems and so are other companies,” says Koelmel. “So now we have to deal with this” (rt.com, 2013) was said for RT. On the one hand, Chevron admits, that virus did not have any huge effects on the company. “I don’t think the US government even realized how far it had spread. I think the downside of what they did is going to be far worse than what they actually accomplished,” Koelmel adds. (rt.com, 2013) Stuxnet is the world's first cyber-weapon of geopolitical significance. Frank Rieger, legendary German hacker organisation Chaos Computer Club calls Stuxnet as “a digital bunker buster”, where the virus represents a new edition to the arsenal of modern warfare. Months later, there is not an Internet security firm, government or even a country which is afraid of its security. Thanks to this, Stuxnet has opened a new era of cyber- war.

Is there a more harmful virus than Stuxnet? Probably yes. Similar to Stuxnet, but still different. More intelligent. And even more sophisticated and dangerous. The process of this virus is still under way to figure out. The origin of another cyber-weapon, Flame, a data- virus, is still unknown. Flame, a virus used to mine documents and communications for secret and sensitive information of Iranian officials. Many scientist thought, that this virus belongs again to the US and Israel (?), with the co-operation of UK (?), however the computer code appears to be at least five years old. Or Flame virus is just more sophisticated? But American officials say that Flame is not a part of Olympic Games. And declined to say or admit whether the United States was responsible for the Flame attack or not. Iran later on warned that the virus was and still is potentially more harmful than Stuxnet. And this is because Flame virus purpose is not to damage the system but to collect different sources and information. On the first sign, the virus appears to have been written by a different group of hackers and programmers, but researchers at Kaspersky Lab in Moscow have proven, that Flame virus is more likely part of the same group as was Stuxnet created. Unfortunately the researchers declined to mention the name of any of the governments. The last discovery was announced in May 2012 by MAHER Centre of Iranian National Computer Emergency Response Team (CERT) with cooperation with Kaspersky Lab and CrySyS Lab of the Budapest University. “Is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found.” (iContact, 2013) Flame can easily spread to other systems over a local network or via memory stick. Is able to record audio- through Skype or MSN, can take screen-shots, is sensible on a keyboard activity. Basically is collecting the information and then sends it on a different command stations and waits for further instructions form the servers. At the end of May 2012, a meeting of computer scientist took place in US regarding the new virus, Flame. Kevin Haley, Symantec's director of security response, talked about an unique virus. “The first thing was its size. The virus is different, way different than anything the company had seen. Stuxnet was really unique because of its size, and this is about 20 times bigger than Stuxnet.” (Kelly, 2012) That time, newly detected virus had “incredible abilities to monitor in- boxes, take screen grabs, even record audio of conversations happening near the computer.” The virus was doing more than some normal program. “There were encrypted pieces, and they had a lot of functionality, so we really started to do some serious investigating.” (Kelly, 2012) The Iranian CERT team believes that there is a close relation between Flame and Stuxnet. Unfortunately till now, we do not have any confirmation- from any

of the sides- if the viruses were launched by US with cooperation of UK or Israel or even with all three of them.

To make a conclusion on this topic is almost impossible. The cyber-world is changing every second and already tomorrow's world can face even more sophisticated and intelligent virus than Stuxnet or Flame. Will the war in cyber-world end in some point? Unfortunately this question is not answerable. The Stuxnet and Flame viruses have proven, that every security is breakable and none of the enterprises or research centres are safe. Unfortunately this includes nuclear weapons. The question is if the world and states are capable to face this war. However the main problem is that there is no internationally applicable definition of cyber-war or cyber-security. "We shall not enter into any of the abstruse definitions of war used by publicists. We shall keep to the element of the thing itself, to a duel. War is nothing but a duel on an extensive scale. If we would conceive as a unit the countless number of duels which make up a war, we shall do so best by supposing to ourselves two wrestlers. Each strives by physical force to compel the other to submit to his will: his first object is to throw his adversary, and thus to render him incapable of further resistance. War therefore is an act of violence to compel our opponent to fulfil our will." (Causewitz, 1989:4) The world has witnessed declarations of war on crisis, obesity, drugs, terror and many other things. If there was a war, we knew who had started it- we could see the soldiers, the progress, the result. But in cyber-war not. We do not know who has attacked us. We cannot see the person or group. Conflicts that are considered to be wars- in cyber world- have never been declared and fought. This problematic is an issue of the 21st century. "This isn't traditional war. The Internet has levelled the playing field, allowing governments that would never launch military attacks on one another to target one another in cyberspace." (Goldman, 2012) If and how is the definition of physical war applicable in virtual environment is the very next question to deal with. Jason Andress and Steve Winterfeld (quoting the same definition) provide gracious answer: "Can these historical concepts be applied to the virtual world? Is the military perspective the right one to look at this problem through? The answer is a declarative: YES" (Andress,Winterfield, 2011:4) To contemplate a little bit further, both geopolitical warfare and virtual conflicts are constructed by human beings. The machines, networks, software do not combat each other out of their free will (yet) as well as bombs do not fly around and destroy whatever they please. What was mentioned in the work of John Arquilla and David Ronfeldt, the possibility of cyber warfare to inflict physical damage to people. Netwar was mostly about damages to other networks- disruptive attacks- although they can wreak havoc and cause significant economic damage (Arquilla, Rondfelt, 2011:44) but in other cases it admits that viruses are able to destroy or corrupt data and cause economic damage and software tools can be used to cause destructive failure in a critical infrastructure like air traffic control, power, or water systems, which can lead to catastrophes (Arquilla, Rondfelt, 2011:45).

Conclusion

The increasing number of cyberattacks on Iran runs to a series of mysterious assassinations and deaths of nuclear scientists. Iran's popularity as a target is increasing every day. And everyone is asking how far can go the cooperation between US and Israel. Super- power warfare has traditionally been dominated by the threat of nuclear attacks, but could cyber weapons change this? Could they be transformed into radioactive

paper weights? Each of the nuclear weapons would need to be highly protected and 100% resistant to viruses for cyber weapons. But as seen in Iran, even the land- based intercontinental ballistic missiles can be easily compromised- and as proven, they do not need to be connected to the Internet. Still, if cyber weapons can be relied upon to stop nations from developing or launching nuclear weapons that would be a good thing. Unfortunately this is the only positive thing about this problematic. And as the science is developing every day, these attacks which were talked about, will not be the last attacks of this kind. Stuxnet and Flame virus have opened new era of Cyber war and only time will show how they will end.

Author is a MA candidate at Aberdeen University and his dissertation focuses on Cybersecurity Defence Strategies.

Reference:

ANDRESS, J., WINTERFELD, S., Cyber Warfare Techniques, Tactics and Tools for Security Practitioners (Elsevier,2011).

ALVI, A., "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", January 2004, accessed October 9, 2013, http://www.academia.edu/1822332/The_myths_and_facts_behind_cyber_security_risks_for_industrial_control_systems

rt.com, "Stuxnet goes out of control: Chevron infected by anti-Iranian virus, others could be next", "RT", last modified November 9, 2013, accessed October 8, 2013, http://rt.com/usa/news/stuxnet-chevron-cyber-virus-348

ARQUILLA, J., RONDFELT, D., Networks and Netwars: The Future of Terror, Crime, and Militancy, (RAND: Santa Monica, CA.,2001).

CLAUSEWITZ, C. On War, (Princeton University Press,1989).

CONWAY,L., "Obama ordered cyber-attacks on Iran's nuclear programme but created a super-virus that is now 'out of control'" "Daily Mail". Last modified June 1 2013, accessed October 9, 2013, http://www.dailymail.co.uk/news/article-2153308/Cyberattacks-Iran-ordered-Obama-created-virus-creating-havoc-internet.html

DAHL,F., "Iran ready to double nuclear work in bunker: IAEA", "REUTERS", November 16, 2012, accessed October 10, 2013, http://mobile.reuters.com/article/topNews/idUSBRE8AF10N20121116?i=2&irpc=932

GLADSTONE and SANGER, "Nod to Obama by Netanyahu in Warning to Iran on Bomb", "The New York Times", September 27, 2012, accessed October 10, 2013, http://www.nytimes.com/2012/09/28/world/middleeast/netanyahu-warns-that-iran-bombmaking-ability-is-nearer.html?ref=world

GOLDMAN, D., "Flame raises the cyberwar stakes", "Security Blogs", last modified May 30, 2012, accessed October 10, 2013, http://security.blogs.cnn.com/2012/05/30/flame-raises-the-cyberwar-stakes/

iCONTACT, "Flame", "iContact" accessed October 10, 2013, http://www.icontact.com/define/flame/

KELLY, S., "Decoding the 'Flame' virus", "Security Blogs", last modified June 5, 2012, accessed October 7, 2013,

http://security.blogs.cnn.com/2012/06/05/decoding-the-flame-virus/

KASPERSKY LAB ZAO, “How to detect a hacker attack”, “SECURELIST”, last modified October 2013, accessed October 2013, http://www.securelist.com/en/threats/vulnerabilities?chapter=38

NASH, E., “Hackers bigger threat than rogue staff”, “VNU Publications”, May 15, 2003, accessed October 10, 2013, http://archives.neohapsis.com/archives/isn/2003-q2/0199.html

NEW YORK TIMES, “Iran’s Nuclear Program. Nuclear Talks 2012” “New York Times”, 2012, accessed October 10, 2013, http://www.physics.ohio-state.edu/~wilkins/energy/Resources/nuclear/iran-nuke-program-NYTopics-2013Jan.txt

ROUSE, M., “Cybersecurity” “WhatIs.com”, last modified December 2010, accessed October 10, 2013, http://whatis.techtarget.com/definition/cybersecurity

The Policy Paper is part of the new CENAA`s long-term program Global Netizenship in Cyber World. It aims to analyse in-depth multispectral and cross-cutting issues of national and international cyber security. Through the establishment of the network of national and international partnerships, CENAA strives to ensure that cyber security will get into focal point of political, corporate and expert elites. Goal of the program is also to uncover the issue of cyber security to all.

CENAA Policy Papers

No. 15/2013, Vol. 2

Centre for European and North Atlantic Affairs

Tolstého 9, 811 06 Bratislava

www. cenaa.org/publikacie/policy-papers/