V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska, Jozef Vyskoč, Maciej Ziarek
Editor: Joanna Świątkowska

Visegrad Fund

The Kosciuszko Institute

V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska,
Jozef Vyskoč, Maciej Ziarek
Editor: Joanna Świątkowska

Visegrad Fund

The Kosciuszko Institute

If you appreciate the value of the presented Report as well as The Kosciuszko Institute's mission, we kindly encourage you to support our future publishing initiatives by making a financial contribution to the association.

V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations
Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska, Jozef Vyskoč, Maciej Ziarek
Editor: Joanna Świątkowska

The publication is co-financed by the International Visegrad Fund (http://visegradfound.org)

Visegrad Fund

Translation: Magdalena Wielgat (chapter 1), Marlena Dobosz (chapter 2), Karolina Gucko (chapter 4), Renata Lasota (chapter 8)

Proofreading: Marlena Dobosz, Karolina Gucko, Bartosz Wójcik

Cover design, layout and typesetting: Małgorzata Kopecka
Print: Dante Media

The Kosciuszko Institute
ul. Lenartowicza 7/4
31-138 Kraków, Poland
e-mail: ik@ik.org.pl
telephone: +48 12 632 97 24
www.ik.org.pl

ISBN: 978-83-93-10-93-6-4

Contents

Introduction

Izabela Albrycht – Chairman of the Board
of the Kosciuszko Institute

Information and communications technology solutions influence every sphere of public and private life and are responsible for the proper functioning of modern states. On one hand, technological advancement has allowed an unprecedented development of civilisation. On the other hand, however, it has led to emergence of new threats, which must become the subject of actions and decisions of entities responsible for the security sphere.

Cyber security knows no boundries – state-level only solutions are not sufficient. In order to meet the cyberthreats, international cooperation is necessary, and the regional alliances, like the Visegrad Group, constitute a key component, while also being a complementation of multilateral cooperation.

The main goal of this publication is to analyse the state of cyber security in Visegrad Group countries and to present recommendations contributing to its strengthening. The Czech Republic, Slovakia, Hungary and Poland are members of the European Union and NATO. Both of these entities have included the activities aimed at protection of cyber space in their agendas. The publication, besides the analysis of activities conducted in this sphere by NATO and the EU, also contains a presentation of possible areas of solidary activities of the Visegrad Group, aimed at further strengthening of cyber security at the international level, as well as within those organisations.

Furthermore, one of the essential purposes of the publication is to familiarise the readers with basic information on cyber space protection and to make them realise how important this area is, from the point of view of each citizen's security. Public awareness of threats is a critical part of prevention in the face of cyberthreats' globalisation.

The publication, by the virtue of its parameters, discusses the most important issues related to cyber security. Each of the chapters is a starting point for further, complex analyses, nevertheless, it constitutes a good portion of knowledge for all interested by this topic and the problems of the modern world security.

All of the analyses are based on public information and focus on non-technical aspects of cyber space protection. The advantage of such approach is accessibility of the text and the possibility to capture the political science's aspect of the cyber security issue. Due to such perspective, the publication is a valuable and useful document for decision-makers, who, on the basis of its recommendations, may address the proper political solutions – both national and international. The report is also a source of practical knowledge for everyone interested in new trends in the field of international security.

While thanking our Partners for cooperation in preparation of the report, I invite you to familiarise yourselves with its contents, and to discuss the issue of cyber security, which has to become, next to economic, energy and military security, a key component of security strategies of particular countries and our "global village".

Selected Theses*

The Kosciuszko Institute

Cyberthreats as a Challenge to the Security of the Contemporary World
Author: Joanna Świątkowska
We currently live in a world where functioning and development of individuals, states and international organisations are based on the use of information and communication technology (ICT) systems. (…) As a result of technological development, apart from significant benefits, there have appeared new types of threats that have to be faced by the international community. One of the most important challenges confronted by states and other entities is to ensure the security of cyber space.

Cyberthreats have revolutionised the way people think about security, they have destroyed the old paradigms concerning the methods of its ensuring and modified the rules that govern international conflicts.

The main dangers related to cyber space are: cybercrime, cyberterrorism and cyberwar.

The above described problems can be overcome only through international and intersectoral cooperation. (…) On this assumption, one of the goals of the present publication is to draw attention to the fact that cyber security should be a common objective, also for the Visegrad Group countries.

Systematisation of Key Cyberthreats
Author: Maciej Ziarek
Since the Internet has become a medium used in almost every domain of life, a risk that it may be used by cybercriminals for conducting attacks and getting illegal profits increases (…). Computer and mobile malware, spam and botnets are clearly part and parcel of the present-day Internet.

Botnets, (…) are networks of infected computers whose owners have no idea that their machines have been attacked. Such an infected computer is commonly termed as a zombie machine. (…) Its use depends on the intentions of its author who is nothing more than a cybercriminal.

Spyware is distinguished by precision. (…) Its purpose is to gather as much information as possible and send it within a specified time period to a server belonging to a cybercriminal.

Nowadays, mobile phones, smartphones and tablets are often equipped with functional and efficient operating systems that allow for advanced interaction with the user and for performing the same tasks as computers (…). Mobile malware is not a myth, nor a fabrication. Its existence is confirmed by statistics.

Spam may be defined as unsolicited emails, for delivery of which a consent has not been expressed.

(…) There is a need to start the IT security education from scratch in order to fight such menaces more efficiently.

Cyber Security in the Czech Republic
Author: Tomas Rezek
Cyber security in the Czech Republic is becoming more and more important as the use of the Internet and ICT systems is on the rise.

Security of private systems is regulated by the state only if the system processes personal data. In such cases, the Office for Personal Data Protection must approve the implemented security measures. After obtaining an approval from the Office, usually no other controls are realised unless there is a security breach. The supervision is rather passive and it relies on the competitiveness in the private sector – unsecure ICT systems in private sector might result in higher costs in case of a security breach. The state steps in only if personal data are involved or if the national security might have been jeopardized.

The control of systems in the public sector is ensured in accordance with the nature of information the systems contain – classified information, personal data, etc. For every new system a security project is created. (…) Moreover, for every risk an emergency plan is created.

The current situation of cyber security in the Czech Republic is very asymmetrical due to the rapid increase of the ICT use in private and now also in the public sector. New systems were already adopted, but an adequate effort to create secure cyber environment has not been made. Theoretical background was created in form of policies and strategies, but the implementation is delayed.

The lack of qualified employees at the key positions in the public sector presents the major challenge for the Czech Republic. Without qualified personnel it would be very difficult to control the implementation of security measures and to govern the cyber space of the Czech Republic. Furthermore, lack of skilled experts may jeopardize international cooperation.

Cyber Security in Poland
Author: Joanna Świątkowska
The responsibility for the Polish cyber security and its protection is diffused. There is no separate entity that coordinates the actions in this area.

"Governmental Program for the Protection of Cyberspace in Poland for 2011-2016" (…) is currently the most important document that plans the actions related to the Polish cyber space (…) its main weakness is that it has not been put into effect since its publication. (…) It should constitute the continuation of the previous Program (for the years 2009-2011), meanwhile, in large part, it is a repetition of the recommendations from the old document.

It can be said that in Poland (…) the implementation of the cyber security steps is being pushed aside or is not executed at all. (…) The decision-makers shift the responsibilities on who should implement essential projects. As a consequence, Poland in reality does not have a functioning cyber space strategy. (…) Moreover, in the presence of the changes introduced in the government administration in 2011, it is not completely clear who is responsible for its implementation.

Poland belongs to a group of countries that notice the process of the militarisation of cyber space. What is more, this country has begun the process of building its capabilities within the scope of conducting military operations in this field.

Paradoxically, the biggest weakness of Poland in the field of cyber security is not the lack of a good preparation for cyberattacks. (…) What really is the biggest offence of some entities (also the crucial ones), is the fact that they do not seem to treat this matter with proper seriousness and probably they do not pay enough attention to treat it with, at least, equal importance as the defence from conventional threats.

There is a need for comprehensive system changes, a need to introduce a body that would coordinate the actions of various other entities which have an influence on the cyber security.

The commitment and collaboration with the public sector is crucial, that is why the cooperation on the basis of private-public partnerships must be intensified. The state should treat the private sector and scientific circles as important partners.

Cyber Security in Slovakia
Author: Jozef Vyskoč
(…) no state-sponsored institution in Slovakia is specialised exclusively in the whole spectrum of cyber security issues. Instead, various state institutions, as well as other organisations, address partial topics related to cyber security.

At the first sight, it appears that Slovakia has a fair amount of coverage of cyber security-related issues – several state bodies are assigned respective roles, there exists basic legislation

and even "The National Strategy for Information Security". The problem, however, is that the mere existence of bodies or documents is not sufficient if even a brief peek at the inside reveals serious defects.

(…) the key document – "the National Strategy for Information Security" (…) is supposed to be of strategic character, this is not the case (…) e.g. key "players" and their interests and possible conflicts are not properly identified (…), it focuses mainly on operation security and technical security issues, completely ignoring important phases of the design, implementation and testing of the IS and the need to respect security requirements there, apparently it considers only "classical" types of systems and completely ignores new trends like cloud computing (…), document represents short-term thinking (…), only "low-level" international cooperation is considered (…).

(…) state institutions addressing cyber security issues seem to be preoccupied with operation security issues and/or questions of jurisdiction – lack of forward-looking thinking on more abstract cyber security issues is visible even for the supposed advisory board (Committee for Information Security).

Professional societies direct their activities mostly towards their members and generally avoid contemplation on more abstract cyber security issues.

(…) though there are visible activities in the area of cyberdefence in Slovakia, these are rather low-level oriented (technical measures, preparation of specialists, etc.). High-level cyberdefence activities, including proper education/training of decision makers on the state level and their connection with executive cyberdefence formations, are missing.

Cyber Security in Hungary
Author: Joanna Świątkowska
Hungary belongs to a group of countries where mainly civilian agencies are in charge of ensuring cyber security, and where the discussion on the militarisation of cyber space is not very advanced.

(…) "National Security Strategy" (…) focuses on unconventional threats, stating that "the risk of an attack against Hungary or its allies with traditional arms is negligible." (…) The document predicts that the number of cyberattacks will multiply in the nearest future and they will become a burning problem, which makes the need for cyberprotection even more urgent. The document recommends that "systems should be strengthened in conjunction with the country's alliance partners, especially those within the EU."

Cyber security was chosen as one of the priorities of the Hungarian Presidency in 2011. (…) The period of the Presidency showed that the country recognises and understands the importance of cyber security. By forming initiatives that are aimed at enhancing international cooperation in this field, not only within the EU but also at a transatlantic level, Hungary presented itself as a country which aspires to take the leading position in promoting cyber security within the EU. (…) One of the most important Hungarian Presidency achievements was the actual progress in the works towards the advancement of the ENISA's operation.

Practical situations, like (…) cyber exercises, exposed imperfections in Hungary's preparation for cyberdefence, showing that there is still a lot to be done. On the one hand, it must be pointed out that Hungary is not an exception and most of the entities are at the beginning of the road towards a solid cyber security system.

Controversial governmental changes and financial burdens which incriminated telecommunications services led to the conclusion that political decisions may prevail over the interest of cyber security. Especially the new rules that concern the governing of the National Agency for Data Protection may result in a loss of trust between the Internet users, which is a fundamental condition for the information society development.

Cyber Security in the European Union: Legal Aspects, Plans, Strategies, Actions
Author: Tomasz Szatkowski
Two important features of the EU approach are its focus on cybercrime and cyberterrorism spectrum of the cyberthreat with a preference for undertakings enhancing the resilience of its critical ICT infrastructure as an implication to its goals of developing the information society.

The Solidarity Clause (Article 222 Treaty of the Functioning of the European Union – TFEU) – another form of mutual commitment, envisaged for mutual assistance of Member States, under the coordination by the intergovernmental mechanisms of the Union, in case of an act of terrorism, man-made or natural disasters, may lend for the EU common action in dimension of countering the cyberattacks.

(…) the legal conditions imply that the overall EU's cyber security capabilities will have "passive" rather than "active" character.

The EU has achieved a considerable merit by providing new standard in the area of penalisation and cooperation against the cybercrime. It has also been active and achieved undeniable progress in the area of enhancing resilience of the Network and Information Security. Its policy and capabilities in cyberwarfare remain very limited with the exception of prospects for funding the research in that area.

NATO Fighting Cyberthreats
Author: Joanna Świątkowska
The NATO's New Strategic Concept introduced in 2010 in Lisbon (…) recommends development of NATO's possibilities in the area of preventing, detecting and defending from cyberattacks and building ability of effective recovery after attacks.

NATO's principal focus is on the protection of its own ICT systems and networks. The Alliance believes that integrity and continuous functioning of its ICT system must be guaranteed in

order to perform its core tasks of collective defence and crisis management. (…) Though "self defence" is a core task, the Alliance's engagement in coordinating member countries' actions for cyberdefence is becoming increasingly visible.

One of those tasks concentrates on implementing cyberdefence into the national activities related to security, including the solutions proposed by the NATO's Defence Planning Process. NATO also develops minimum requirements for those national networks that are connected to or process NATO information.

At present, the most important provision, on the Alliance's response to cyberattack upon any of NATO members (…) says that in case of an attack, any collective defence response is subject to decisions of the North Atlantic Council. In addition, NATO shall provide coordinated assistance to any Ally being a victim of a cyberattack.

The Smart Defence initiative can be very attractive in the context of building capabilities associated with cyber space. It provides a chance for close cooperation which promotes share of information, experience and, what is very important, collective development of technological solutions. (…) Building a joint Visegrad Group countries "front" within NATO, which would specialize in cyber security, is therefore worth considering.

NATO is a political and military alliance which now has the chance to play the key-role in the field of cyber security, especially in regard to cyberterrorism and cyberwar.

*Footnotes referring to the passages from the *Selected Theses* can be found later in the text.

1. Cyberthreats as a Challenge to the Security of the Contemporary World

Joanna Świątkowska

We currently live in a world, where functioning and development of individuals, states and international organisations are based on the use of information and communication technology (ICT) systems. Information has become one of the most desired assets while the practically unlimited communication possibilities, introduced by the latest technological developments, have irreversibly changed the reality. Those unprecedented phenomena also have a huge impact on the changes that took place in the security sphere. As a result of technological development, apart from significant benefits, there have appeared new types of threats that have to be faced by the international community. One of the most important challenges confronted by states and other entities is to ensure the security of cyber space. Considering the fact that the implementation of the ICT solutions is directly related to the socioeconomic development, it is necessary to emphasize that the tendency of their further use will still be rapidly growing.

Cyberthreats have revolutionised the way people think about security, they have destroyed the old paradigms concerning the methods of its ensuring and modified the rules that govern international conflicts. The very attempt at defining cyberthreats and at determining their essence proves problematic, not to mention their efficient prevention. For several years now, politicians, experts and scientists have been debating on establishing one version of the key terms that are related to the threats coming from cyber space. Due to space constraints, the polemic of various conflicting opinions is omitted from this publication in favour of preliminary definitions in order to familiarise the reader with the subject matter and with the issues discussed in the present paper.

The fundamental task faced by the entities responsible for the security of contemporary communities and states is to ensure cyber security. Both European and American literature defines this term mainly in relation to the process of reaching a required level of protection of the information processed by the ICT systems and networks by providing three elements: confidentiality, integrity and availability.[1] Therefore, cyberattacks shall be defined as hostile

1 National Institute of Standards and Technology, The Cyber Security Coordination Task Group, U.S. Department of Commerce, *Smart Grid Cyber Security Strategy and Requirements*, Draft NISTIR 7628, September 2009 see also: § 3 para. 1. of the Regulation of the Prime Minister of 25 August 2005 on the basic requirements for ICT security, Chapter 2. 1., (Dz. U. 2005 nr 171, poz. 1433 ze zm. / Journal of Laws 2005, no. 171, item 1433 with changes).

activities threatening the information protection understood as above. However, this "traditional" approach applies only to data protection. In order to tackle other threats and to better reflect the current (and the expected) situation, the definition needs to be extended. Thus, a factor that is equally important to data protection is the protection of proper systems functioning. Therefore, the issue of defence against abuse of systems for illegal and harmful activities needs to be underlined.

Cybercrime and Cyberterrorism

The main dangers related to cyber space are: cybercrime, cyberterrorism and cyberwar. However, the boundaries between these phenomena are fluid and difficult to discern, if only because of the fact that each of those acts can be carried out with the use of the same methods and instruments. As a consequence, it is not only difficult to prevent the attacks and to prosecute the entities responsible for a given act, but also to punish the perpetrators.

According to the definitions elaborated at the 10th United Nations Congress, held from 10 to 17 April 2000, cybercrime may by understood in two ways. In the narrow sense, it is "every illegal activity conducted in the form of electronic operations that is aimed at compromising the security of computer systems or data processed by those systems". In a broad sense, it is "every illegal activity committed by means of, or related to, computer systems or networks, including i.a. illegal possession and sharing or dissemination of information with the use of computer systems or networks".[2] Money or private data theft and child pornography are just a few examples of cybercrime. It is worth noticing that in 2010 organised banking crime cartels earned more money through online banking fraud than drug cartels from the sale of their products.[3] Therefore, apart from social consequences, cybercrime has disastrous effects on national economies and on the financial condition of private companies.

The phenomenon of progressive informatisation of crucial elements responsible for the functioning of the most important areas of the contemporary states favours the emergence of new threats. ICT solutions are responsible for proper functioning of a number of elements of the critical infrastructure, including i.a. the systems related to the energy, water supply and gas infrastructure. The consequences of a cyberattack aimed at those assets may be tragic: from financial losses, disorganisation and paralysis of citizens' lives to tangible damage to a given infrastructure. All this leads to a situation where cyberattacks may become a particularly desirable instrument for cyberterrorists. The proposed definition of cyberterrorism refers to "a politically motivated attack or a threat of an attack on computers, networks or IT systems aimed at destroying infrastructure and at intimidating or imposing far-reaching political and social aims on governments and citizens".[4] There is also an opinion that the world has not experienced a real act of cyberterrorism yet. There is just more emphasis on the fact that the Internet and ICT networks are currently used mainly for recruitment, mobilisation, exchange of information and coordination of terrorist actions. The majority of experts, however, are of the opinion that acts of cyberterrorism are just a matter of time and everything should be done to prevent and to be prepared for them.

ICT tools have many features which facilitate cybercriminal and cyberterrorist activity. These include, among others, low input costs required for conducting an attack and relative anonymity. It is difficult not only to physically identify the perpetrator of a given attack, but also to bring them to justice. This issue is directly related to the jurisdictional problems associated with cyberthreats, which are new enough that the system of justice and the legislative framework often prove inadequate to properly prosecute and punish the perpetrators. What is more, certain countries have not recognised the problem of cybercrime yet and they do not respond efficiently enough to such activity.[5] As it can be seen, cybercrime may be committed from anywhere on the Earth, including areas where they are not treated as punishable acts by the authorities.[6]

The above described problems can be overcome only through international and intersectoral cooperation. Above all else, jurisdictional systems of countries should be harmonised to efficiently prosecute and punish the aggressors as well as to develop information exchange platforms, which will allow not only better preparation against cyberattacks, but also more efficient neutralisation.

In the context of both promotion of the need for closer cooperation and the critical information infrastructure (CII) vulnerability, yet another issue should be mentioned. Currently, a major part of the ICT systems, including those used by the public sector, is owned or operated by private entities. Therefore, it is not possible to protect the safety of cyber space without close cooperation with this sector. Exchange of information and close cooperation are necessary. The problem occurs though at the stage of building trust and awareness of co-responsibility for cyber security. The private sector is fearful of sharing sensitive information. They do that reluctantly all the more that such information is often related to dangers threatening their products and services.[7] Very often the point of view of the private sector is not understood by the public entities. This assumption can be illustrated by the following example: in order to provide efficient defence against cyberthreats, the present-day states face a challenge of determining the regulations governing certain activities and "codes of conduct" in cyber space. Some states call for the need to impose solutions protecting the security of cyber space upon other entities, including those belonging to the private sector. Despite the fact that those decisions

2 M. Nowak, *Cybernetyczne przestępstwa – definicje i przepisy prawne*, Poznan School of Banking, http://www.ebib.info/2010/113/a.php?nowak, [access: 04.04.2012].

3 Deloitte, *Cyber Espionage. The harsh reality of advanced security threats*, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_sp_cyber_espionage_screen_friendly_100511.pdf, [access: 04.04.2012].

4 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, 2005, p. 36.

5 Those places are called "paradises for cybercriminals".

6 But this is complicated even further. For instance, an attack may be conducted in a way that makes it virtually impossible to discover the perpetrator as in the case where infected computers of unaware users are used to attack successive ones.

7 There is also a risk of appropriation of their solutions by competitors.

affect the private entities, decision-makers tend not to recognise the need to consult those entities and engage them in the process of creating the necessary solutions. Those problems should be overcome as soon as possible.

In the context of cyberthreats, the matter of trust may be also seen from a different perspective. Establishing and maintaining trust in Internet communication is a serious undertaking, in particular if too many actors are involved in the process, not to mention the fact that the mechanisms used these days are not easily scalable, which makes them inappropriate for dealing with such a complex task. In the light of recent incidents of hacking and in view of the negligence on the part of certification authorities, reliance on hundreds of such entities, which are included in the browsers' lists of "trusted" CAs, may be questionable.[8]

Another aspect related to ICT solutions, especially to the Internet, is the specificity of the base project, the idea based on which the network was built. The project came down to the easiest possible access to the network and to the possibility of its co-creation by the users themselves. At the very beginning, security was not considered to be an important aspect that would require particular attention. As a result, at present it is much easier to hack into a system than to protect it. Additionally, this vulnerability is magnified by a lack of user awareness regarding the threats facing them and by the absence of basic rules of cyber hygiene related to the use of the Internet and of ICT tools. It is especially dangerous in face of the rapidly growing trend of their application. During the last years, an increase in use of such devices as smart phones and tablets can be observed. Almost everyone has them and keeps using them without even being aware of the threats which are related to their use. Furthermore, solutions such as cloud computing, which are particularly vulnerable to threats, are more and more popular. All this should become a subject of particular attention and security measures. Convenience must go hand in hand with security.

Cyberwar

One of the most controversial categories related to the attacks in cyber space is cyberwar. The process of cyber space militarisation progresses increasingly in spite of the fact that a number of commentators and experts are of the opinion that it is more of a component accompanying a conventional war than an independent phenomenon. Even if we assume that the cyberattacks conducted against Estonia (2007) or Georgia (2008) did not deserve to be referred to as "cyberwar", it is undeniable that the observed behaviour of present-day states lead to more and more dangerous cyberconflicts. The category of cyberwar is the most difficult one to define. It breeds the highest number of conflicts. For the purposes of this paper, it is proposed to define cyberwar as a form of information warfare, that is "an external activity of a state, organised in the form of violence, leading to achievement of specific political goals and aimed at destroying or modifying the communication systems of an opponent or the information passing through these systems, as well as at protection of own information systems against similar actions by the opponent".[9]

An increasing number of states introduce the necessity to formulate solutions allowing for defence against attacks performed by other entities (including those state-controlled) coming from the cyber space into their military doctrines, and they focus more and more often on building offensive capabilities related to performing the attacks. Additionally, we are witnessing a large-scale process of formation of military organisational units suitable for performing activities in the cyber space.[10]

A classic example of a country developing their operational capacity in the cyber space is the United States, which has not only established a special military command dedicated to ensure cyber security (U.S. Cyber Command), but also, by including the cyber issues in its military doctrine, it has recognised cyber space as the fifth dimension of warfare.[11] Another interesting example is Estonia, where the first volunteer cyberarmy, composed, among others, of engineers and employees of banks and other corporations, was established. They dedicate their time to help to protect the Estonian cyber space. In case of cyberwar, the volunteers will answer to military command.[12]

Cyberwar radically modifies the traditional understanding of conflicts and the way of ensuring security. Security is no longer thought of in the categories of classical attempts at keeping the balance of power while the perception of the concept of deterrence and the effectiveness of retaliatory actions have changed. All this is a consequence of at least several reasons. One of them is the fact that the destructive attacks that do originate from state actors may never be proved or assigned to particular countries, which is known as the problem of attribution. Cyberattacks could, for example, be performed by individual units that are actually sponsored or supported by countries, but it is all but impossible to prove such dependency.[13]

Additionally, a problem related to absence of the commonly approved "code of conduct" in case of hostile actions of countries in the cyber space should also be emphasized. The Geneva Conventions regulate certain activities related to conduct of conventional wars. There is no similar international agreement that would apply to military operations in cyber space. For example, should two countries at war, capable of attacking each other's

8 *DigiNotar Hacked by Black.Spook and Iranian Hackers*, http://www.f-secure.com/weblog/archives/00002228.html, [access: 04.04.2012].

9 T. Jemioło, P. Sienkiewicz (eds), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka)*. Volume I, Research report, Warsaw 2004, pp. 74-75, K. Liedel, P. Piasecka, Wojna cybernetyczna – wyzwanie XXI wieku, http://www.geopolityka.org/index.php/analizy/987-wojna-cybernetyczna-wyzwanie-xxi-wieku, [access: 04.04.2012].

10 Those divisions are commonly called cyber armies.

11 BBN, *Terroryzm cybernetyczny – zagrożenia dla bezpieczeństwa narodowego i działania amerykańskiej administracji*, Warsaw, 2009, p. 8.

12 *Pierwsza armia Internetu*, http://www.wykop.pl/ramka/587495/pierwsza-cyberarmia-na-swiecie-estonska-liga-obrony-cybernetycznej/, [access: 04.04.2012].

13 Once again it is worth to recall the example of Estonia. During the attacks against this country, massive traffic originated from such different sources as the United States, China, Vietnam, Egypt and Peru despite that many facts indicated that they were inspired by the Russian Federation (which, by the way, has never been proved). Source: J. R. Westby, *The Path to Cyber Stability, in: Rights and responsibilities In cyberspace. Balancing the need for security and Liberty*, EastWest Institute, p. 2.

ICT infrastructure, not be banned from attacking and, say paralysing hospitals?[14] Potential building of agreements or treaties will be impeded at least because of the problematic issue of distinction between offensive and defensive capabilities of countries. Despite this, these issues undoubtedly await resolution, either through formulation of new legislation or by adapting the existing one. The matter needs to be deeply discussed at the international level.

At the same time, it should be remembered that the introduction of regulations and restrictions in the name of lofty goals should not limit either privacy of users or their freedom of expression, which constitute the main advantages of activities in cyber space. Even if this turns out to be necessary, it should be first widely discussed how and to what extent the regulations should limit the rights of cyber space users.

ICT tools allow promotion of various convictions, ranging from those related to human rights or to democratic ideals to less noble ones. In addition, popularisation of ideas may take a dangerous form. Hacktivism is a term which defines the activity related to hacking into computers for promotion and manifestation of political views. Despite of the fact that it is not always considered in its own right as cybercrime, its consequences may produce illegal and disastrous effects. Theft of personal information, damage to systems (happening upon acts of hacking), disclosure and publication of sensitive data as part of a protest – all that can accompany the activity of hacktivists and it may have extremely dangerous consequences.

Other Aspects

To summarise the above problems, it is worth to mention the example of Stuxnet virus, considered as the most advanced virus in the world. Stuxnet attacked the Iranian nuclear power plant, taking overall control of critical computers and successfully paralysing its operation.[15] Experts emphasize that Stuxnet is one of the most perfectly prepared and the most damaging viruses. There are many indications that it was created on demand of a state entity.[16] The virus showed that the limit of technical capabilities related to illegal penetration of ICT systems is constantly shifting and touches more and more critical objects. It is not only difficult to defend against threats, but also to hold perpetrators liable for their performance.

According to a number of specialists, human is the weakest link in cyberdefence. It is the human factor – human mistakes, lack of knowledge and caution as well as unhygenic use of ICT devices – which leads to the most common problems. Scratching PIN on credit cards or using weak passwords are common mistakes and acts of negligence. Additionally, an unaware and inadvertent Internet user may fall victim to malicious software and their computers may then be used for illegal purposes (as part of a group of infected computers forming the so-called botnet). This is an especially threatening phenomenon due to the fact that it can turn innocent citizens into accomplices to crime without them even being aware of it.

However, a human may also be an intentional intruder who conceals his or her real intentions, enters a system gaining trust and knowledge, and then uses them for illegal purposes. Such activities are related to the next category of cybercrime, that is cyberespionage. One of its variants is industrial cyberespionage, which not only causes huge financial losses, but is also exceptionally difficult to detect. A commonly known situation related to Wikileaks shows how far-reaching consequences for public safety, including that of public entities, a leak of confidential information may have: from loss of prestige, through erosion of authority to a severe security threat.

Another threat comes from increasingly popular social networks, which are frequently used as a tool for successful spreading of disinformation and also as a source of harmful applications.

It should be emphasized that cyberthreats have multiple sources, beginning with flaws and technical actions, through infection of hardware at the stage of production, hacking into systems and manipulation, right up to infiltration of the structures of the attacked entity by people with dual identity.

According to media reports from the Gulf War, the United States damaged the military systems of Iraq using a virus installed on printers that were delivered to Iraq as part of a standard hardware order.[17] This illustrates the necessity to look after the whole "chain" related to the use of ICT solutions, starting from the project stage, through manufacturing, up to considering the human factor. Among the solutions capable of increasing security, it is worth to distinguish such measures as education, raising awareness and application of international standards in the context of technological solutions.

To conclude the review of the most dangerous problems resulting from the use of cyber space, it is also important to notice the potential consequences, which could arise from accidents and failures, whether they are intended or not. As an example, the EastWest Institute raised an issue of increasing dependence of the global network and its infrastructure of undersea cables that carry over 99% of intercontinental Internet traffic to mobile devices connected to the Web. The results of cable damage, the access to which is very difficult, may have enormous consequences.[18] When considering the problem of cyber security, it is important to be aware of such threats.

14 More: B. Rooney, *Calls for Geneva Convention in Cyberspace*, http://blogs.wsj.com/tech-europe/2011/02/04/calls-for-geneva-convention-in-cyberspace/, [access: 04.04.2012].

15 It was achieved by exploiting the holes in the Windows operating system.

16 *Stuxnet, najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu?* http://swiat.newsweek.pl/stuxnet--najgrozniejszy-wirus-swiata--czy-to-dzielo-izraelskiego-wywiadu,65632,1,1.html, [access: 04.04.2012].

17 D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, p. 6.

18 Mobilizing for international action, Second Worldwide Cybersecurity Summit in London, EastWest Institute, http://www.worldwidecybersecuritysummit.com/, [access: 04.04.2012].

This short overview of threats resulting from the use of cyber space is only an outline of the problem. However, it leads to at least one substantial conclusion. It is not possible to protect the cyber space without international and intersectoral cooperation. It is a basic condition for facing threats that constantly increase in intensity, evolve and know no bounds. On this assumption, one of the goals of the present publication is to draw attention to the fact that cyber security should be a common objective, also for the Visegrad Group countries. Of course, global actions are necessary, but the regional ones should supplement them.

By analysing the cyber security issues in particular V4 countries, including their good practices and weaknesses, we wish to prove that joint operations, exchange of information and solidary conduct of politics on the international scene, especially in the EU and NATO, may bring great benefits. Such cooperation is particularly important in times when expenses for defence, especially in the areas related to unconventional threats, are commonly reduced.

2. Systematisation of Key Cyberthreats

Maciej Ziarek

In the last few years, the Internet has become so commonplace that more and more households decide to purchase a broadband Internet connection the moment they buy computer equipment. As far as enterprises and institutions are concerned, they would not be able to transfer data efficiently without access to the Internet. A computer connected to the Internet provides its users with many more opportunities than one without a constant connection. Unfortunately, cyber space is not free of menaces. The present paper aims at systematising the biggest threats that may be encountered by Internet users around the world, as well as at discussing the effects of the attacks undertaken by cyberterrorists.

Networks Of Infected Computers – Botnets and Zombie Computers

Malicious software (in short: malware) can get into an operating system in a number of ways. It may be sent via an email message as an attachment or through an instant messenger, or come from such sources as software that appears to be useful at first sight, an infected USB flash drive or a website initiating a download of code while loading. In the latter case, users are frequently unaware of the fact that something has ever been downloaded to their hard drive. One of the attacks that is based on such a principle is the so-called "drive-by download" attack. When it happens, the user does not see any notifications on the screen and all is done without their acceptance. What is more, it suffices to visit a prepared malicious website to initiate downloading.

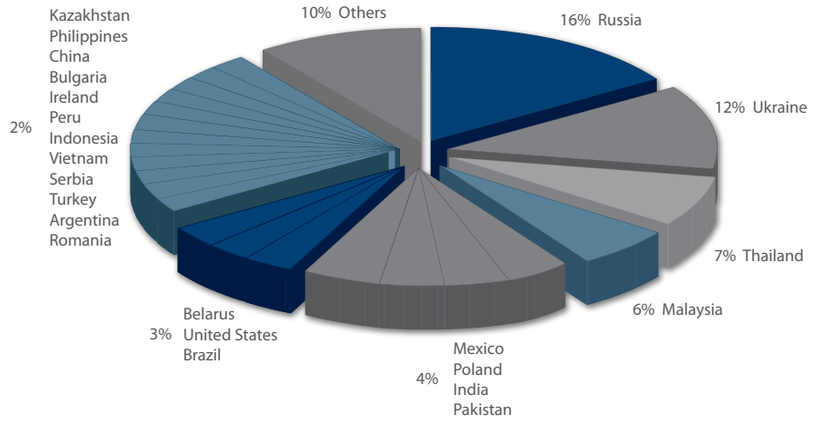
Not every virus or Trojan horse works the same way. Their functions differ depending on the intentions of their authors. Some malicious software make its presence felt from the very beginning of the infection: there appear some unknown applications on the list of installed software, the user is annoyed with notifications popping up every now and again on the screen and it takes longer than usual for the operating system to load. One of the things the user will decide to do first in such a case is to scan their PC with antivirus software. But at times, the bug does not signal its destructive activity, and for a reason. Botnets, which are referred to in this section of the text, are networks of infected computers whose owners have no idea that their machines have been attacked. Such an infected computer is commonly termed as a zombie machine. And a single botnet can include tens or even hundreds of thousands of such machines. Its use depends on the intentions of its

author who is nothing more than a cybercriminal. They may sell a part of the processing speed of the botnet on the black market or use it to send spam or to initiate the so-called DDoS attacks (Distributed Denial of Service attacks) to cause temporary or permanent server deactivation.

But how a computer can get infected? The zombie computers that belong to a botnet are usually infected with a net worm, a specific kind of malware that can replicate the same way a virus does and does not need any data carrier in order to move and infect successive computers. What is more, net worms exploit gaps in software in order to secretly get into the operating system. After their installation on a new computer, a net worm connects it to the botnet without its owner even being aware of it. All zombie computers can be activated by the malware owner, and the processing power and the Internet connection of the infected computers can be then used for illegal purposes. At this time, the user may notice temporary slow-down in their computer's performance. In most cases, botnets consist of tens of thousands of infected machines. Such a number is most optimal for the criminal as it makes a botnet easier to hide. However, every so often huge botnets made up of hundreds of thousands of infected machines are discovered.

One of the most dangerous functions of a botnet is a possibility to carry out DDoS attacks. Each website is maintained by a server fitted for this purpose. This hardware has certain resources and technical parameters such as a processor and RAM memory that may be allocated in response to certain requests made by Internet users (e.g. attempts at loading a website). If a server receives a large number of such requests at short intervals, the system may become overloaded, in which case the service will be denied. It is dangerous because with such a great number of zombie computers it is quite easy and efficient to block websites of government institutions or the ones having millions of visitors a day. A country that has really felt the effects of DDoS attacks was Estonia, which has experienced a series of massive cyberattacks since May 2007, where the servers of the National Assembly, banks and government agencies were blocked. As a result, Estonia has been practically cut off from a number of Internet services. This situation shows how important it is to protect the cyber space of each country.

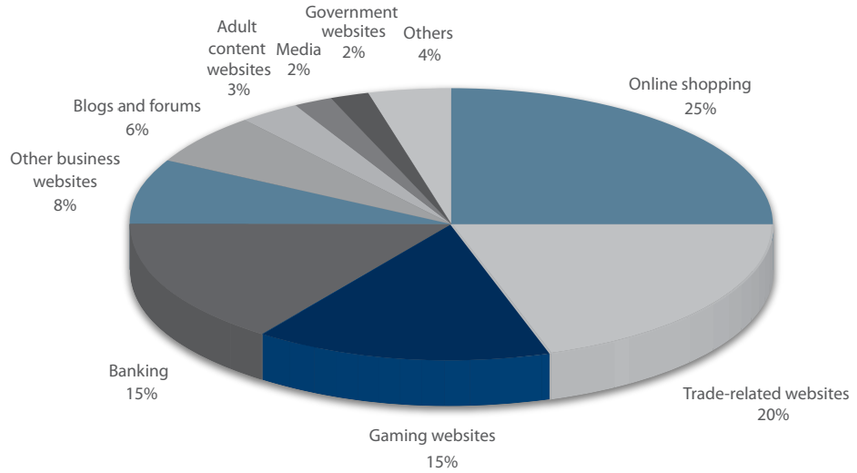
Fig. 1. Distribution of DDoS attack sources by country – second half of 2011



In the second half of 2011, 201 countries experienced cyberattacks and 90% of these attacks came from 23 countries listed on the above diagram. The geographical distribution of DDoS attack sources has undergone a visible change as compared to the first half of 2011. Previously, the top positions were occupied by:

- the United States – 11%,
- Indonesia – 5%,
- Poland – 5%.

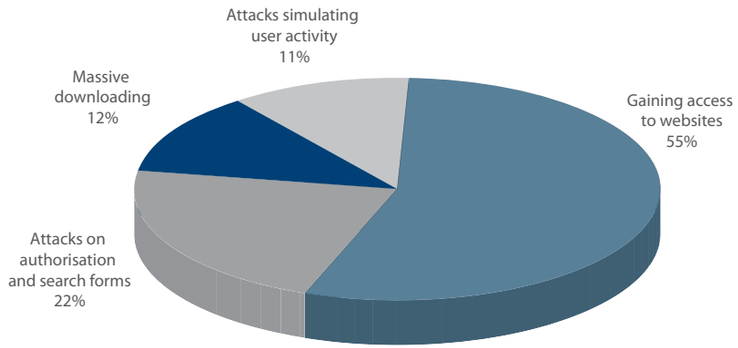
Fig. 2. Distribution of attacked websites by area of activity – second half of 2011



In the future, the number of DDoS attacks will increase. It is associated not only with an increase in sales of computer equipment but also with faster Internet connections providing greater bandwidth capacity and giving cybercriminals a possibility to use their botnets more efficiently. The average strength of DDoS attacks discovered in the second half of 2011 was measured at 110 Mbit/s, which means a 57% increase as compared to the first half of 2011.

Botnets used for DDoS attacks may bring huge profits to cybercriminals. The best example is their influence on the securities market. Different informative websites, which record changes on the market and among the companies operating on the stock exchange, may fall prey to the attacks happening after publication of reports capable of delivering substantial profits. All so as to enable cybercriminals to keep some information for themselves and use it to take steps (e.g. to purchase or sell shares) in order to make profit through fraudulent means. An attack like this took place on 10 August 2011. It was directed at the Hong Kong securities market, which is responsible for publishing important information on the major stock market traders. As a result of the attack, the trade in shares belonging to seven giants had to be suspended for a whole day, which caused unimaginable losses. After an investigation, it turned out that the person behind the attack was a 29-year old businessman playing the stock exchange.

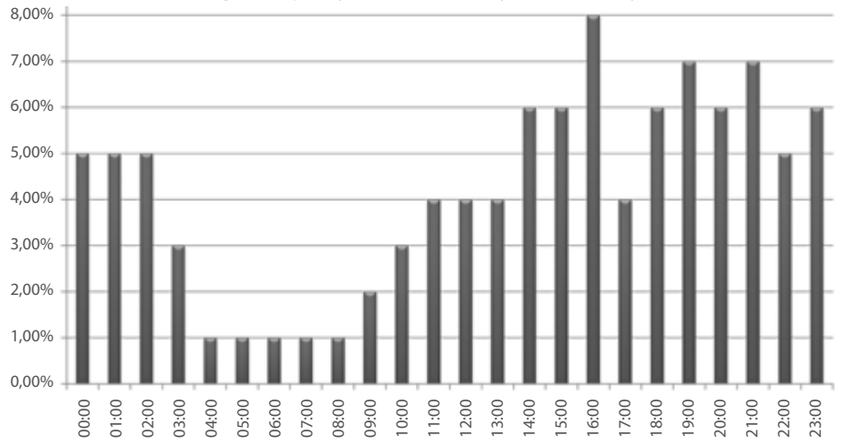
Fig. 3. Types of HTTP Flood attacks – second half of 2011



The above diagram shows a version of the so-called HTTP flood attack, one of the most frequent DDoS attacks which consists of sending a large number of HTTP requests (the same as the ones sent while accessing a website) to an attacked server. The HTTP Flood attacks account for 80% of all the cyberattacks. According to the diagram, 55% of the attacks of this type are based on an attempt of a botnet to get access to a given website. Another method of accessing a website is based on using different forms of authentication. It is less popular but still common. The third type of an HTTP Flood attack is making an attempt at downloading the same file multiple times.

The last diagram on botnets demonstrates that the periods of highest activity (in terms of attacks) coincide with daily routines of an average Internet user: they are activated around 9 a.m., when a large number of users start their computers at home or at work, and they are deactivated around 3 a.m.

Fig. 4. Frequency of DDoS attacks by time of the day – the second half of 2011



The best way to avoid having a computer incorporated into a botnet is to observe a few basic security procedures such as:

1. Having installed antivirus software that:
   a) is monitoring activity of applications in real time;
   b) automatically updates malware signatures on a regular basis;
   c) informs the user about potentially dangerous actions on the part of computer programs.
2. Having installed and activated a firewall preventing unauthorised programs from accessing the Internet.
3. Being careful while visiting websites that are not included in the so-called white list of safe and acceptable resources.
4. Spam filtering.
5. Updating the operating system and all the applications installed on the computer.

All the statistical data used in the present report have been obtained by means of a botnet activity monitoring system (used at Kaspersky Lab's antivirus laboratory) and Kaspersky DDoS Prevention technology.

Global and Local Attacks

Another menace is spyware, which is an equally threatening issue as botnets. Spyware is distinguished by precision. It does not aim at connecting computers to a botnet, nor at making fun of people by changing their keyboard layout. Just like net worms, which infect the operating system in order to connect a PC to a botnet, spyware works covertly. Its purpose is to gather as much information as possible and send it within a specified time period to a server belonging to a cybercriminal. The data collected by spyware includes in particular:

- credit card numbers and expiry dates;
- usernames and passwords;
- captured emails;
- and information on the visited websites.

Spyware is a type of malware that is supposed to collect data related to such domains as Internet banking. Contrary to the common belief, spyware is a very simple application that can take print screens the moment a user clicks the mouse or log all the keystrokes typed on the keyboard. More advanced forms of spyware can also track users' activity on the most popular social networks such as Facebook.

And this happens globally. A cybercriminal tries to infect as many machines as they can in order to increase their chances for getting valuable information and making instant profits. Antivirus software deals with spyware applications really well. However, just as it is in case of a botnet, the antivirus software has to be automatically updated on a regular basis and be allowed to track the activity of the running software and to prevent users from downloading malicious code from infected websites. A global attack means also that the malicious code is placed on a number of different servers so as to enable cybercriminals to store the data even after one of the servers is closed.

Global attacks pertain to every computer connected to the Internet. But what effect do they have on corporations and institutions? They are certainly vulnerable to these attacks. However, they are also prone to another threat, namely local attacks, also known as targeted attacks, where a cybercriminal targets a given company and customises the malware in a way so as to penetrate its resources as efficiently as possible. Piece by piece, they gather information on their target in order to be able to bypass the protections used by the victim. They search for such information as the date of antivirus signatures included by some antivirus applications in the emails sent from the company. With the information on the type of software used by a given institution, a cybercriminal does not have to adapt their malware for different possible scenarios, so they can focus on the software that is actually used by the victim.

In some cases cybercriminals attack a company only for a specific purpose, for instance, to obtain information that can be useful for attacking another company. Such an attack was conducted in 2011 on RSA organisation. The people behind the attack stole the data related to the SecurID tokens used as an additional form of authorisation in a number of institutions, including government ones. A person having such data and a token ID is able to clone the token. Shortly after the attack on RSA, the cybercriminals used the cloned token to attack Lockheed Martin, a company supplying the American Army with equipment. The data needed to bypass the second form of authorisation, that is the login and the password, were probably stolen with the help of some social and technical manoeuvres that could have been performed on the company's staff. The above example demonstrates how the security of one company can influence that of other organisations and institutions. The essence of targeted attacks is that the attacker reaches their goal little by little. It is pertinent to highlight that traditional (massive) spyware would not have sufficed in this particular case.

However, that does not mean at all that spyware has never been used for industrial espionage. The Stuxnet worm, which attacked the computers having PLC drivers used in refineries and power plants, is one of the best examples of such activity. It has become clear that cybercriminals were interested in spying the economies of certain countries. The largest number of infected computers was recorded in Iran. Another malware that seems to have gone down in the history of targeted attacks is Duqu, which is even more mysterious. It is a Trojan which does not cause any damage to hardware but concentrates mainly on stealing information and data stored on the infected machines. It is very mysterious: until quite recently, it has been difficult to even classify certain elements of its code. Since new and new versions of Duqu appear on the Web all the time, the cybercriminals seem to be constantly developing their "work" and trying to make it more and more difficult to detect.

Mobile Devices and Airborne Threats

Nowadays, mobile phones, smartphones and tablets are often equipped with functional and efficient operating systems that allow for advanced interaction with the user and for performing the same tasks as computers. They are currently used for:

- checking email;
- connecting to various websites (while staying permanently logged in);
- storing information on marketing plans and strategies (corporate smartphones).

These three points are important because, in case of a malware infection, they provide access to critical information. Mobile malware is not a myth, nor a fabrication. Its existence is confirmed by statistics:

Fig. 5. Number of mobile malware signatures (as of February 1, 2012: 5,320.)

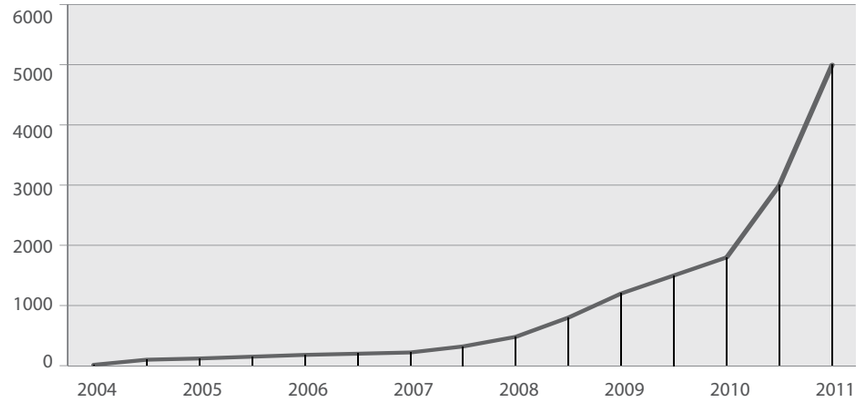
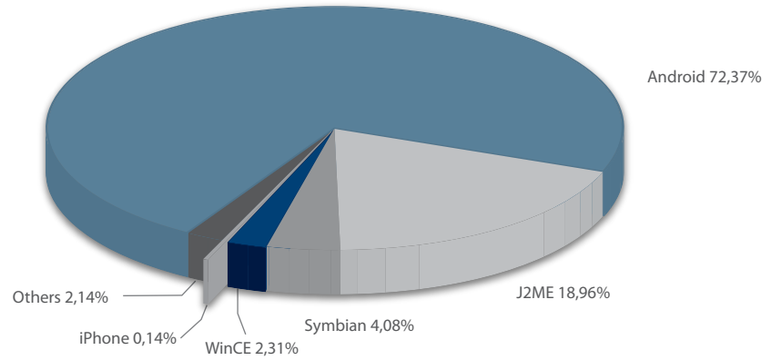


Fig. 6. Number of malicious software applications designed for specific platforms (as of February 21, 2012)



As it can be seen, mobile threats are on the increase. Their most frequent victim is Android, the leading mobile operating system these days. This did not escape the attention of cybercriminals. The most frequent threat to all the mobile operating systems is an SMS Trojan. First, a user downloads a program from an unofficial source because they think that it is a useful application. Then, right after its launching, the application starts sending text messages to premium numbers. In most cases, users have no idea that they have been attacked until they check their telephone bill and spot a preposterous amount to pay. Unfortunately, cybercriminals become more and

more impudent and there are still cases where a malicious application is found even at official online stores belonging to the very manufacturers of operating systems. Such a situation may be particularly dangerous when a user trusts that no malware can appear on official store websites. That is why it is important to always verify what system processes an installed application requires access to. If it is making phone calls or sending texts messages, it should raise our suspicions.

What is interesting, there is not much malware that is designed for Apple iOS operating systems. It may be credited to the company's policy carried out from the very establishment of the App Store. All the applications available there are checked by Apple. In addition, devices having an iOS operating system do not have administrator rights, due to which malicious software cannot cause severe damages to a device.

One of the most serious incidents that affected the owners of mobile operating systems was related to the sector of Internet banking. It involved the ZeuS Trojan which attacked the Windows operating system while its user was logging in their bank account and it replaced some of the elements displayed on the screen so as to make the user give their full login and password instead of a masked password. Next, the user was redirected to a website where they had to download a certificate to their mobile phone. It was supposed to improve the security of online transactions. In reality, it was malware and it directed all the text messages, including those coming from the bank and containing single use mTAN passwords, to the cybercriminal immediately after its installation. In such a way, one of the safer forms of authentication has been bypassed: single use passwords sent in text messages are no longer safe.

Spam and its Influence on the Work of Institutions

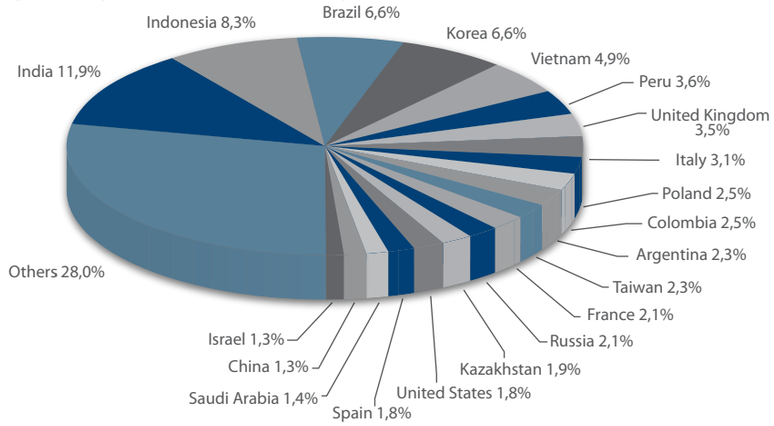
Spam may be defined as unsolicited emails, for delivery of which a consent has not been expressed. The end part of the definition is important because the mailing sent by websites whose Terms of Service, including the provisions on sending email offers concerning a given website or service provider (e.g. a free email account provider), we have accepted cannot be considered as spam.

For dispatch of unwanted emails, spammers most frequently use the above mentioned botnets. Email addresses of spam receivers are collected in a number of ways. Some of them are found on the Internet on discussion forums and newsgroups using automated software. It suffices that a user publishes their email address on the Internet and a robot will automatically find it while browsing websites and add it to the spammer's contact list. However, spammers tend to send advertisements to random addresses hoping that a part of emails will get to real email account owners. It is very important not to ever respond to spam. Otherwise spammers will add the address of the respondent to the list of confirmed addresses and the amount of spam he or she receives will only increase.

In the long term, both companies and individuals may feel uncomfortable receiving large numbers of unsolicited emails. Among the consequences of receiving spam, the following can be distinguished:

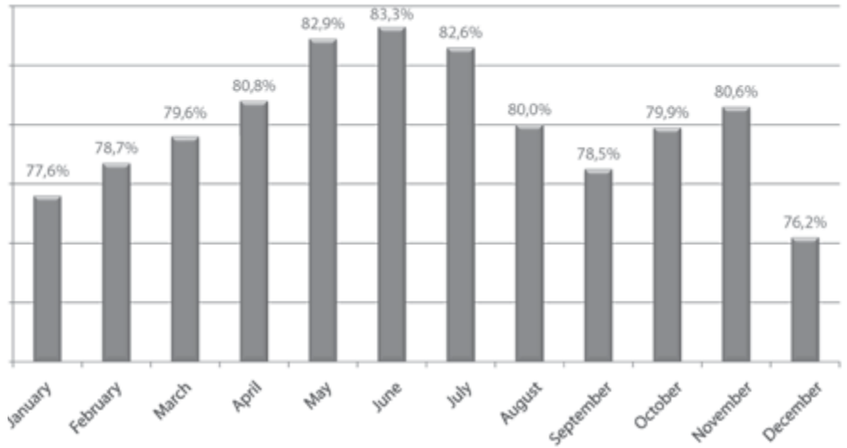
- waste of time on email sorting;
- necessity to constantly remove spam;
- risk of accidental removal of a non-spam email;
- danger of visiting a website containing malicious software or a dangerous attachment;
- risk of falling for a spam offer (less experienced Internet users);
- unnecessary use of hardware resources (both on the part of the client and on the part of the server);
- generating artificial Internet traffic;
- excessive use of Internet connection, which is particularly acute for users of mobile devices.

Fig. 7. 20 largest spam sources in February 2012



The consequences which seem to be the most serious are: risk of computer infection, risk of accidental removal of an important message and waste of time on fighting against junk email. A corporation which overlooks an email from a client may not only miss out on a chance to make a profit but also lose its reputation.

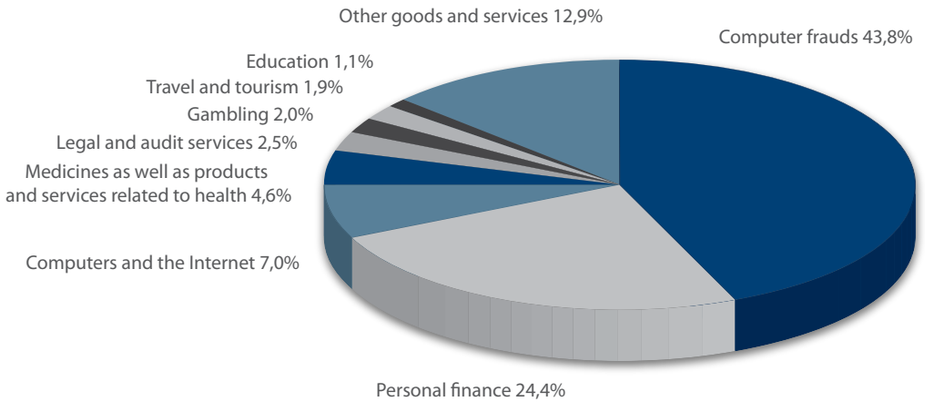
Fig. 8. Volume of spam in email traffic in 2011



The above diagram shows the percentage share of spam in email traffic in 2011 by month. Spam generates email traffic in an artificial way because it does not contain any valuable content or

attachments addressed to a given person but it is essentially composed of advertisements. Unfortunately, there was no month where the share of spam in email traffic would be smaller than three quarters of all the emails sent around the world. But this fact points to yet another important issue. At Christmas time, spammers do not generate much more email traffic than in other months. So why are Internet users warned against Christmas spam and threats related to it as soon as in November? Apparently, it does not mean that the amount of spam increases in that period. What happens is that spammers modify the content of messages and their contact lists. This is why the diagram does not show any significant increase in spam email traffic in this period.

Fig. 9. Spam by category in February 2012



Conclusion

Since the Internet has become a medium used in almost every domain of life, a risk that it may be used by cybercriminals for conducting attacks and getting illegal profits increases. The aim of the present paper was to raise awareness of the scale of the problem. Every day, millions of individuals and institutions all around the world face the problems mentioned throughout this study. Computer and mobile malware, spam and botnets are clearly part and parcel of the present-day Internet. As a result, there is a need to start the IT security education from scratch in order to fight such menaces more efficiently.

3. Cyber Security in the Czech Republic

Tomas Rezek

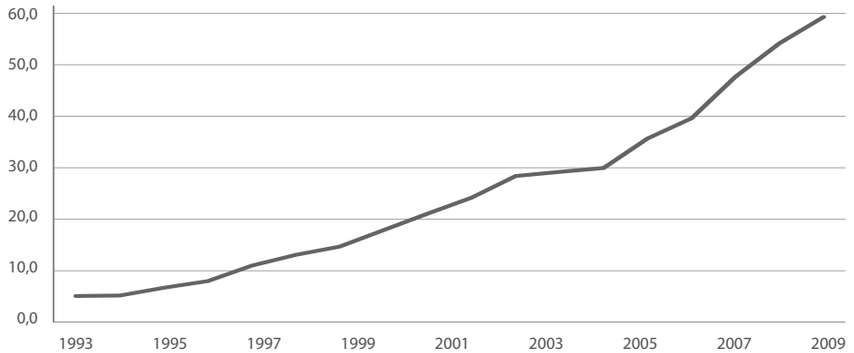
Introduction to Cyber Security in the Czech Republic

Cyber security in the Czech Republic has become an important issue of national security after year 2001. It is true that potential risks related to use of the Internet were present even before, but they were relatively small in comparison with other security issues like organised crime or corruption. Growing interest in cyber security in the Czech Republic is related to increasing dependency on the Internet and on ICTs (information and communication technologies). This dependency arises from pursuing efficiency in private and public sector – web applications, online communication and other benefits of the Internet usage motivate companies and governments to use the Internet and ICTs in order to cut costs or to improve offered services. Nevertheless, this trend requires increase in cyber security as well, because this dependency creates potential risks for governments. The use of the Internet and growing dependency has not been developing in the same way in every sector.

Households and Cyber Space

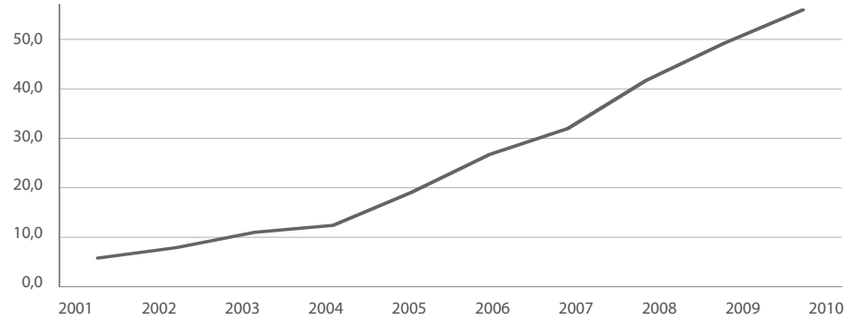
The number of Internet users, PC owners and generally the ratio of dependency on the Internet was relatively low before the year 2000. The following chart illustrates the number of PC owners in the Czech Republic during the last twenty years.

Fig. 1. Households with PC (%). Source: Czech Statistical Office, http://www.czso.cz/



From the perspective of cyber security, viruses and violation of legal property due to illegal program distribution were the main issues of the '90s in the Czech Republic. As we can see on the following chart, a rather dynamic growth of connectivity to the Internet started in year 2004, since then the average growth has been 10% every year. Rapid growth of households connected to the Internet resulted in growing cybercriminality, as there was a growing number of potential victims.

Fig. 2. Households with Internet connections (%). Source: Czech Statistical Office, http://www.czso.cz/



It has been twenty years since the beginning of the Internet era in the Czech Republic. At the beginning, only one company was providing Internet connection to companies or households (it was privatized in 2006 and became a part of Telefonica O_2). Today, there are more than 800[1] companies providing access to the Internet, mainly *via* WiFi. Nevertheless, the largest Internet provider is still Telefonica O_2 with more than 80%[2] market share in 2010, followed by T-Mobile, UPC and other companies.

Private Sector and Cyber Security

Private companies with foreign owner or partner had easier access to cyber security standards and defence measures. This allowed them to be prepared for potential attacks; on the other hand, the implementation of such measures might have created extra costs in comparison with the other companies without the proactive cyber security approach. We can divide security measures in companies into two groups – internal and external. The internal security measures were introduced in order to defend internal networks, systems and data within a company. The external security focused on communication with clients, suppliers, public administrations and other external entities. An example of the internal security standard can be the requirements for a password to access a system – specified minimal length, etc. As an example of the external security measures, we can take secured websites for payment and order processing – a confidence loss of clients generally leads to a loss of clients. The requirements for the private sector regarding cyber security depend on their business field, but generally they arise only from law (see below).

1 The total number of Internet providers presented on the webpages of http://rychlost.cz/isp/, [access: 07.04.2012].

2 Stated in article about fixed internet connection, J. Peterka, 2010, http://www.lupa.cz/clanky/kabel-opet-porazi-adsl/, [access: 07.04.2012].

Responsibility of Public Sector

Cyber security is a very serious topic especially in relation to the public sector. Not only does the government create the legal and organisational framework for cyber security, but it also governs the immense amount of personal data and other sensitive information. Moreover, the state is the most likely target for potential cyberattacks with political motivation. The majority of the IT systems in the public sector are a part of countries' critical infrastructure, because they govern the pension benefit system, health register, social insurance system, etc. Again the question of cyber security in the public sector is strongly related to the use of the Internet and to the dependency on the Internet and ICTs.

In the '90s, every ministry or other state body was running its own or shared local network – an intranet or LAN. These networks were separated from the Internet and remote access was, at the beginning, reserved only for emergencies. Therefore, the security measures focused on protection of access points to an intranet. However, the trend at the end of '90s in the Czech Republic was to make the public sector more effective. In pursuit of this goal, certain IT services were outsourced to private companies. Systems started to be connected to the Internet in order to allow more comfortable access to the public. New web applications were designed to facilitate the interaction between the state and individuals. A connection to the Internet also allowed more efficient cross-department communication and data sharing. The recent events only highlight this trend and its potential danger. This year, the Ministry of Labor and Social affairs deployed a new system for the payout of social benefits and allowances. Originally, different allowances were paid out by different offices, now there is a single office responsible for the payout of all social benefits and allowances. Originally separated systems were operated by the state, but new system is operated by a private company. The potential risks are even higher as the database with personal data is not stored on dedicated servers, but in the cloud.

The following table illustrates services provided by some governmental bodies in year 2010. These services are of rather basic nature. Nevertheless, it suggests that security measures have to be implemented in order to secure the provision of listed services. Despite the nature of the services, they might be targeted by cyberattackers (DoS, DDoS, data fraud, data loss, etc.).

Table 1. Services provided by governmental bodies in 2010. Source: Czech Statistical Office, http://www.czso.cz/

Total	Information for Life Situations		Application Form for Download		Application Form Online		Complete Online Submission	
	Total	%*	Total	%*	Total	%*	Total	%*
Ministries	12	85.7	13	92.9	7	50.0	5	35.7
Courts of Law	82	90.1	38	41.8	32	35.2	62	68.1
State Prosecutors	9	100.0	1	11.1	0	0.0	0	0.0
Job Centers	67	97.1	68	98.6	53	76.8	42	60.9
Geodetic and Land Registries	19	90.5	21	100.0	7	33.3	6	28.6
Sanitary Stations, Veterinary Stations	21	95.5	17	77.3	5	22.7	2	9.1
Other	116	98.3	84	71.2	30	25.4	32	27.1
Total	326	94.8	242	70.3	134	39.0	149	43.3
*Percentage from total participating organizations								

The following table presents the security measures used by different governmental bodies in 2010. Despite a high percentage in every category, the list of security aspects is not complete in order to accept the premise that public sector in the Czech Republic has strong and sufficient cyber security.

Table 2. Security measures used by different governmental bodies in 2010. Source: Czech Statistical Office, http://www.czso.cz/

Bodies of the State	Organization using:							
	Virus-detection Program		Hardware or Software Firewall		Regular Data Backup		Electronic Signature	
	Total	%*	Total	%*	Total	%*	Total	%*
Ministries	13	92.9	13	92.9	13	92.9	13	92.9
Courts of Law	96	99.0	79	81.4	97	100.0	97	100.0
State Prosecutors	10	100.0	8	80.0	10	100.0	10	100.0
Job Centers	76	100.0	68	89.5	76	100.0	76	100.0
Geodetic and Land Registries	22	100.0	19	86.4	22	100.0	22	100.0
Sanitary Stations, Veterinary Stations	29	100.0	25	86.2	29	100.0	28	96.6
Other	127	100.0	118	92.9	121	95.3	121	95.3
Total	373	99.5	330	88.0	368	98.1	367	97.9
*Percentage from total participating organizations								

Legal Framework

From the legal point of view, two major laws influence cyber security measures in the Czech Republic apart from other laws, which have their impact on the cyber space as well (like criminal law, for instance). It is the law No. 101/2000 – Personal Data Protection Act and law No. 365/2000 – Information Systems in Public Sector Act about information systems in the public sector. These two legal acts present the basis of legal framework in the Czech Republic for cyber security.

Personal Data Protection Act[3]

The main aim of this act is to unify the legislation of the Czech Republic with the European Community and to exercise everyone's right to the protection from unauthorised interference with privacy, also to regulate rights and obligations in processing of personal data and specify the conditions under which personal data may be transferred to other countries. This law creates legal structure for the Office for Personal Data Protection, which is in charge of executing this act.

The act applies to any subject dealing with personal data, with the exception of strictly listed cases like protection of national security etc. The act distinguishes three categories of personal data – personal data, sensitive data and anonymous data. To each category applies different constraints and obligations for data processing, data storage and data transfers.

This act influences cyber security in regard to personal data. It states under what conditions personal data can be kept and processed. The link between cyber security and this act is indirect. In case of security breach caused by a cyberattack that violates conditions stated by this act for dealing with personal data, the Office for Personal Data Protection will take action. Given this causal connection, the Office does not have to remain passive. Based on the premise that cyber security is crucial for ensuring personal data protection, the Office may declare security standards and other measures to ensure sufficient protection of personal data. It is true that personal data may not be always involved when there is a cyber security breach. Therefore it does not guarantee high security standards in all cases, but it responds to the most sensitive scenarios of cyberattacks.

Information Systems in Public Sector Act[4]

This act defines information systems and their use in the public sector. It also declares the necessary characteristics that the information systems have to possess with regard to their functions. This means interface characteristics, data availability, certification authorities, process of certified information distribution, etc. More importantly, it also specifies the roles of particular subjects. The administrator of information systems in the public sector is the state. On the other hand, the operator of the system might be a private legal entity, unless it is against the law (when the system deals with classified information or communicates with military systems, etc.). The operator is responsible for the security of the system.

The Ministry of Interior is the most important actor – it formulates long term policies regarding information systems. It approves concepts from public administration and it is also responsible for long term definition of security policies concerning information systems in the public sector. The public administration is responsible for implementation of security measures defined by the Ministry. For the purpose of security, the Ministry issues regulations that have to be adhered to. Particular security measures based on high level regulations are the responsibility of the public administration. The act states that the concept and implementation of security measures have to be adequate to the nature of the system.

This act on cyber security in the Czech Republic influences particularly organisational aspects. It declares that the administrator must be the state. The responsibility to define high level security concepts is on the Ministry of Interior. The application of these concepts is the responsibility of the public administration. The public administration also has to specify adequate security measures to implement. The security of the system itself is the responsibility of the operator. A very important aspect of this act is the influence on the consecutive systems. The information systems of independent entities are partly subject to the regulation if they are connected to information systems in the public sector.

Documents and Strategies

The following documents and strategies present determination of Czech government to prepare ground for safer cyber space.

National Strategy for Information Security of the Czech Republic[5]

This document assures implementation of best practices and cooperation between public and private sector in order to establish secure ICT systems in the Czech Republic. Conclusions in this strategy are

3 *Personal Data Protection Act*, http://www.legislationline.org/documents/action/popup/id/6854, [access: 07.04.2012].

4 *Information Systems in Public Sector Act*, http://www.szrcr.cz/uploads/download/zakon_365_2011_v_aktualnim_zneni.pdf, [access: 07.04.2012].

5 *National Strategy for Information Security of the Czech Republic*, www.govcert.cz/ViewFile.aspx?docid=21667318, [access: 07.04.2012].

further elaborated in "the Action Plan for Implementation of Measures from National Strategy for Information Security of the Czech Republic" (approved by government resolution number 677/2007). National strategy was formulated by the Ministry of Interior in 2005.

Priorities declared in this strategy are:
- Management of information security and risk management;
- Awareness about information security;
- National and international cooperation on information security;
- Implementation of best practices in information security;
- Protection of human rights and freedom;
- Competitiveness of Czech economy.

Security Strategy of the Czech Republic[6]
This key document was approved by the government in 2011 and it defines the main interests of the Czech Republic in cyber security. It highlights the potential danger created by the increasing dependency on information technology. Cyberattacks are placed on the same level with other security issues – terrorism, weapon of mass destruction proliferation, regional conflicts, etc. This strategy reflects not only the security issues relevant to the Czech Republic, but also issues related to the international partners – NATO members, EU member states, etc. It also declares that security of ICT systems related to critical infrastructure is a key governmental priority. The creation of national Computer Security Incident Response Team (CSIRT) is one of the declared tools for achieving this goal. The strategy declares an intention of the Czech government to create ICT system capable of rapid restoration of functionalities.

This document is very important as it declares cyber security as one of the main priorities of the government and it clearly states the intention of the government to actively participate in the protection of national ICT systems. Other, more specific documents and policies are based on this strategy.

Cyber Security Strategy of the Czech Republic for Years 2011-2015[7]
This strategy further elaborates on "the Security Strategy of the Czech Republic". It defines interests of the Czech Republic with regard to cyber security. The main goal of cyber security strategy is the protection of ICT systems in the Czech Republic and mitigation of potential damage caused by cyberattacks. This document is the basis for the creation of policies, legal acts, resolutions and other norms. Basic principles of the strategy are:
- Coordination and intensification of cooperation between private, public and academic sector;
- Individual responsibility;
- Private sector responsibility;
- Cooperation between departments;
- International cooperation;
- Suitability of adopted measures.

6 *Security Strategy of the Czech Republic*, 2011, Ministry of Foreign Affairs, http://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_strategie_cr/index.html, [access: 07.04.2012].

7 *Cyber Security Strategy of the Czech Republic for years 2011-2015*, 2011, Government of the Czech Republic, www.govcert.cz/ViewFile.aspx?docid=21667315, [access: 07.04.2012].

Main goals declared by the strategy are:
- Strengthening cyber security of ICT in public sector and of critical infrastructure;
- Establishing a Computer Emergency Response Team (CERT) department on the governmental level in the Czech Republic;
- International cooperation;
- Cooperation between public, private and academic sector;
- Increasing awareness of cyber security.

Action Plan for Cyber Security Strategy of the Czech Republic for Years 2011-2015[8]
The action plan declares particular measures which need to be implemented in order to meet the goals declared in the strategy. The goals and measures are classified in seven chapters (see below). It clearly links a given goal to relevant tasks, responsible body and expected date of completion. This plan is updated every year with current progress within every chapter.

Chapters of the Action Plan:
1. Cyber security coordination and risk management.
2. Support of international cooperation in the field of cyber security.
3. National cooperation between public sector, private sector and academic sector in the field of cyber security.
4. Creation of legislative framework to improve cyber security in the Czech Republic, protection of human rights and freedom.
5. Increasing the awareness about cyber security in the Czech Republic.
6. Increasing cyber security in ICT in public sector and in communication infrastructure of the Czech Republic.
7. Strengthening resilience of ICT systems against cyberattacks.

Strategy for Creating CERT Departments in the Czech Republic[9]
This document describes the current situation regarding the CERT department creation in the Czech Republic. It also declares a target model of CERT departments' organization within the Czech Republic and in regard with global CERT network. The strategy describes processes, how CERT department should deal with potential cyberattacks.

Organizations and Cooperation

Ministry of Interior[10]
The Ministry of Interior has main influence on cyber security standards in the Czech Republic. The Ministry defines long term goals related to security of information systems.

The Ministry politically promotes the cyber security issues within the state. Furthermore, it is also responsible for international cooperation concerning cyber security. The Ministry participates

8 *Action Plan for Cyber Security Strategy of the Czech Republic for years 2011-2015*, 2011, Government of the Czech Republic,www.govcert.cz/ViewFile.aspx?docid=21667318, [access: 07.04.2012].

9 *Strategy for Creating CERT departments in Czech Republic*, 2011, Ministry of Interior, www.govcert.cz/ViewFile.aspx?docid=21667314, [access: 07.04.2012].

10 Ministry of Interior, http://www.mvcr.cz/, [access: 07.04.2012].

in negotiations with other countries within international organisations. The Ministry of Interior represents the Czech Republic in the Committe on Information, Communications and Computer Policy within the OECD. It also represents the Czech Republic at ENISA (European Network and Information Security Agency). Two board members of ENISA are Czech delegates (Management Board Member and Alternate Management Board Member). They are responsible for ENISA's budget and program approval. National Liaison Officer is another representative within ENISA responsible for monitoring information and network security in the Czech Republic and for communication with other Liaison Officers.

The Ministry is partially responsible for the cooperation within the European Union (together with the Ministry of Foreign Affairs). This cooperation is mainly within the Convention on Cybercrime. The delegates of the Czech Republic signed the Convention in 2005. However, it has not been ratified yet.

Ministry of Defense[11]
The Ministry of Defense cooperates in the field of cyber security within NATO. The Czech Republic, despite being a NATO member, is not a member of NATO Cooperative Cyber Defense Centre of Excellence. Nevertheless, a representative of the Ministry signed a memorandum with NC3A (NATO Consultation Command and Control Agency) in 2010 to open the way for closer cooperation in the development of advanced technologies to meet the 21st century security challenges.

Office for Personal Data Protection[12]
The Office is responsible for personal data protection regardless of the nature of the system. Therefore it influences the cyber space security standards, when personal data are involved. The Office cooperates with other local institutions.

Police
According to the criminal law, violation of cyber security leads to legal prosecution. The Police of the Czech Republic has dedicated offices that deal with cybercrime. These specialised units provide necessary information for other police units.
In order to fight cybercrime, the police also share information and coordinate investigations with partner organizations from other countries (the Interpol, foreign police forces etc).

GOVCERT.CZ[13]
GOVCERT.CZ is an acronym for the Governmental Emergency Response Team, which was established by the Ministry of Interior. It is a government platform for cyber security and functions as a protection centre of the Czech Republic. The portal has not been completed yet, but in the future it should provide a framework for secure and reliable use of the Internet and ICTs. The portal is also a central communication tool for reporting cyber incidents at government level.

Currently, the GOVCERT.CZ is not operational and the functions are performed by CSIRT.CZ (see below). GOVCERT.CZ is responsible for communication with other CERT organisations worldwide. It also coordinates activities together with other institutions in the Czech Republic as well as abroad in case of a serious cyberattack. Nevertheless, GOVCERT.CZ is not a member of the European Government CERTs group.

CSIRT.CZ[14]
CSIRT.CZ is a Computer Security Incident Response Team of the Czech Republic. The team coordinates solutions of security incidents in computer networks in the Czech Republic. The CSIRT.CZ concept was created in 2007 and since 2010 (effectively 1.1.2011) consists of four part-time experts from nongovernmental organisation CZ.NIC. CZ.NIC serves CSIRT.CZ on the basis of mutual agreement[15] between the Ministry of Interior and CZ.NIC. The agreement ends by June 2012. By this date the management of the CSIRT.CZ must be fully under the Ministry of Interior.

Other Institutions

- **The Security Information Service**[16]
  It acquires, collects and evaluates information of major impact on the security of the country, protection of its constitutional setup and economic interests. Therefore its activities cover cyber security as well, but mainly in wider context of national security.

- **National Security Authority**[17]
  NBU is responsible for personnel and facility security clearance procedures. It has overall competences in the area of the protection of classified information (including supervision and methodology). NBU also carries out a certification of technical means, information systems, cryptographic devices, cryptographic sites and shielded chambers; develops and approves national cipher algorithms and creates a national cryptographic protection policy; issues security standards on the protection of classified information.

Current Situation

Cyber security in the Czech Republic is becoming more and more important as the use of the Internet and ICT systems is on the rise. This change took place in the private sector in the '90s. During the last ten years it has been the public sector that started to take the advantage of the Internet and ICT systems in order to achieve higher efficiency and to reduce costs. Legacy systems in the public sector have been replaced by modern web applications and new ICT systems. This development creates a need for skilled employees, who are able to manage those systems and to ensure their proper functioning. Despite the benefits that new technology brings, it also creates potential risks. Therefore, it is necessary not only to implement new systems and technologies, but also to create secure environment – in this case secure cyber space.

11 Ministry of Defense, http://www.army.cz/, [access: 07.04.2012].
12 Office for Personal Data Protection, http://www.uoou.cz/uoou.aspx, [access: 07.04.2012].
13 GOV CERT CZ, http://www.govcert.cz/default.aspx, [access: 07.04.2012].
14 CSIRT.CZ, http://www.csirt.cz/, [access: 07.04.2012].
15 *Memorandum on CSIRT of Czech Republic*, http://www.csirt.cz/files/nic/doc/Memorandum_CSIRT.CZ-en.pdf, [access: 07.04.2012].
16 Security Information Service, http://www.bis.cz, [access: 07.04.2012].
17 National Security Authority, http://www.nbu.cz/cs/, [access: 07.04.2012].

Security of private systems is regulated by the state only if the system processes personal data. In such cases, the Office for Personal Data Protection must approve the implemented security measures. After obtaining an approval from the Office, usually no other controls are realised unless there is a security breach. The supervision is rather passive and it relies on the competitiveness in the private sector – unsecure ICT systems in private sector might result in higher costs in case of a security breach. The state steps in only if personal data are involved or if the national security might have been jeopardized.

The control of systems in the public sector is ensured in accordance with the nature of information the systems contain – classified information, personal data, etc. For every new system a security project is created. In such project, the security of the systems is assessed from different points of view – natural disaster, terrorist attack, disruptions in energy supply, cyber security, etc. The implemented security measures have to be adequate to the probability of the risk. Moreover, for every risk an emergency plan is created.

The current situation of cyber security in the Czech Republic is very asymmetrical due to the rapid increase of the ICT use in the private and now also in the public sector. New systems were already adopted, but an adequate effort to create secure cyberenvironment has not been made. Theoretical background was created in form of policies and strategies, but the implementation is delayed. As an example, we can take the creation of the CERT department. The main issue is the lack of qualified employees in the public sector (like in the case of CSIRT). To create a secure cyber environment, the police need more specialists to be able to successfully tackle cybercrime, the public administration is in need of professionals who would be able to design and to manage processes supporting secure cyber environment, and also skilled staff to actually use the newly implemented systems.

The lack of qualified employees at the key positions in the public sector presents a major challenge for the Czech Republic. Without qualified personnel it would be very difficult to control the implementation of security measures and to govern the cyber space of the Czech Republic. Furthermore, lack of skilled experts may jeopardize international cooperation. This issue might become critical in the near future, when the use of cyber space and of ICTs in public space will increase. Consequently, the risk of cyberattack against the critical infrastructure will become more probable combined with potential damage, which could be caused by a cyberattack. Increasing use of ICTs in all sectors of the society also increases the need for functional international cooperation, which is crucial to secure the cyber space.

4. Cyber Security in Poland

Joanna Świątkowska

The examination of the Polish cyber security issues needs to be looked at taking into account two aspects. The first one is the analysis of the existing state of affairs, including the activity of the entities responsible for cyber security or the actual effectiveness of the introduced solutions. The second perspective is taking into consideration the evaluation of the planned actions included in the most important strategic documents related to national security. From the 'here and now' point of view, what matters is the current country's preparedness for cyberattacks, although having regard for the fact that the protection of cyber space generally constitutes a relatively new sphere of security of the modern countries, it is necessary to focus on strategic future plans. The present article contains a review of the most important issues from both perspectives and gives a comprehensive view only when they are considered together. By virtue of restrictions on the length of this publication, it is a primary analysis requiring further development – on the one hand it exposes the most important issues related to cyber security in Poland, and on the other hand it constitutes a starting point to the recommended more detailed prospective research.

Cyber Security in the Most Important Defence Strategies

The 2007 "National Security Strategy of the Republic of Poland" (NSSoRP), which defines vital interests of Poland in the field of security, in the part concerning challenges and threats, emphasizes the dangers that follow the use of cyber space. The document notices a direct relationship between the cyber security and the country's proper functioning, including its economic development and possibilities to run effective operations in the military sphere. This strategy pays attention to the necessity of critical information infrastructure protection (CIIP) and ensuring the security of classified information. The most important recommended actions that lead to the improvement of cyber security include the need for close cooperation between the public and private sectors, which share the responsibility for cyber space, and the international cooperation, in the first place with the European Union (EU) and NATO.[1] Although the strategy determines the fundaments for building the national security system,[2] the biggest problem lies in the low level of implementation of the postulated solutions.

1 More: *National Security Strategy of the Republic of Poland*, Warszawa 2007.

2 The national security system considered "as a sum of powers, measures and resources destined by the country to realise the tasks in the field of security, properly organised for these tasks, maintained and prepared, from which a management subsystem and a number of executive subsystems are distinguished" – according to the Strategy of Development of the *National Security System of the Republic of Poland 2011-2022*, p. 3.

A remedy for this weakness is to be reached by another document: the "Strategy of Development of the National Security System of the Republic of Poland 2011-2022".[3] Its main goal is to improve the effectiveness and cohesion of the Poland's national security system, including cyber security. The document details and develops the issues related to cyber space protection in Poland, indicating the country's role in this field. An important rule is a subsidiary governmental help for the private sector, the key sector in context of ensuring cyber security. A reflection of this kind of approach appears, *inter alia*, in the critical infrastructure protection (CIP) system, which also embraces some elements of the information and communication technologies (ICT) systems. The obligation to take care of the critical infrastructure (CI) security rests on its operator or owner, and the country's role amounts to the coordinating and supervising function. An intervention of the national entities should only take place in crisis situations, when the private entities' actions are not sufficient and they do not guarantee security.[4] Nevertheless, a system constructed in this way has its weak points. The biggest problem is the lack of possibility to audit and control the implementation of the postulated security features.[5] It is, therefore, extremely important to conduct the activities that would involve private entities in conscious infrastructure protection, ensuring thereby a thorough and responsible performance of duties.

NSSoRP concerns more than just civil aspects related to cyber space. It notices the progressive and irreversible trend of informatisation of the Polish army, indicating the necessity to introduce solutions that would also protect it from cyberattacks. In this aspect, it is recommended to develop the operational abilities of the entities that are especially dedicated to the protection of the defence department's ICT systems.[6]

The same strategy announces the creation of a comprehensive "Cyberspace Security Policy of the Republic of Poland" in the first half of 2012.[7] This document is to be completed on the basis of the already existing "Governmental Program for the Protection of Cyberspace in Poland for 2011-2016" (hereafter: the Program), which is currently the most important document that plans the actions related to the Polish cyber space.

The Program recommends the actions that will lead to preventing and fighting cyberthreats and it includes suggestions for legal, organisational, technical and educational operations. Furthermore, the aim of the Program is to identify the entities responsible for cyber security and specify their competences, build a coherent risk evaluation system for public entities (which would also include guidelines for private entities), create a system for operation coordination, threat counteraction and prevention as well as cooperation and information exchange with partner countries, international organisations and, above all, with the private sector.[8]

Other recommended solutions intended to improve cyber security include the creation of the Interministerial Coordination Team for Protection of Cyberspace of the Republic of Poland (pol. Międzyresortowy Zespół Koordynujący ds. Ochrony Cyberprzestrzeni RP), responsible for the coordination of the operations related to Polish cyber security and the supervision of bringing the realisation of the tasks imposed by the Program to an end.[9] The project also assumes legislation changes that would adjust the terminology of basic categories related to cyber security (e.g. concerning cybercrime), solve the problems of the responsibility for the Polish cyber space protection and putting into order the measures necessary to pursue the perpetrators.[10] Additionally, the Program suggests appointing a Government Representative for Protection of Cyberspace of the Republic of Poland (pol. Pełnomocnik Rządu ds. Ochrony Cyberprzestrzeni RP) and a representative of the head of an organisational unit for cyber space protection in public administration entities, as well as creating a similar post for the private entities.[11]

The Program contains a number of interesting recommendations but its main weakness is that it has not been put into effect since its publication. Available information indicates that the status of this document, which is directed to ministerial arrangements, has not changed so far. Moreover, in the presence of the changes introduced in the government administration in 2011, it is not completely clear who is responsible for its implementation. The current Ministry of Interior, that is the former Ministry of the Interior and Administration, states that the body responsible for the infrastructure and which should take care of putting the Program into effect is, since its creation, the Ministry of Administration and Digitalization. This one, however, still in January 2012, did not give an answer whether and, if so, when it was going to take care of the matter.[12] The lack of an entity responsible for the implementation of the Program's resolutions makes the document basically useless and calls into question the probability of creation of the necessary "Cyberspace Security Policy of the Republic of Poland". Additionally, another problem indicated by the experts arouses controversies: the Program was not consulted enough during its creation. It needs to be emphasised that in case of such a specific matter, this situation should not have taken place.[13]

Finally, the mistake that is found in the Program must not be ignored and unnoticed. This crucial document, from the point of view of building Polish cyberstrategy, contains a factual error which is hard to explain as an oversight, and it can be a symptom of a bigger problem consisting in underestimating the importance of cyber security and not paying enough attention to building its protection. The Program says that "Poland has ratified the Council of Europe Convention of 23 November 2001 on Cybercrime",[14] while on 29 March 2012, it turned out that the information does not correspond with the facts: Poland is a signatory of the Convention, but it has not ratified the document yet.[15] The mistake still has not been corrected, despite the fact that the document was

3 Ministry of Defence, *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2012-2022. Projekt*.
4 Ibid., p. 39.
5 Ibid., p. 101.
6 Ibid., p. 119.
7 Ibid., p. 133.
8 *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016. Wersja 1.1*, Warszawa 2010, p. 8.
9 Ibid., p. 9.
10 Ibid., p. 15.
11 Ibid., p. 16.
12 Gazeta Prawna, *Rząd zapomniał o cyberbezpieczeństwie*, 2012, http://www.gazetaprawna.pl/wiadomosci/artykuly/587082,rzad_zapomnial_o_cyberbezpieczenstwie.html, [access: 29.03.2012].
13 Ibid.
14 *Rządowy program ochrony cyberprzestrzeni* . . . , op. cit., p. 11.
15 *Convention on Cybercrime status*, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, [access: 29.03.2012].

announced about two years ago. All those remarks lead to the conclusion that Poland currently does not have any document actually in force which would be a comprehensive strategy related to cyber space protection.

Review of Entities that Protect Polish Cyber Space

The responsibility for the Polish cyber security and its protection is diffused. There is no separate entity that coordinates the actions in this area. Therefore, distinct institutions are partially responsible for particular areas related to cyber security. The presented review of the entities that protect Polish cyber security is divided into three parts. First, the entities dedicated to public administration cyber security will be analysed, then, the analysis will be focused on the entities that act mainly in respect of private users, and finally, separately, the national defence sphere will be presented in detail. Obviously, this division is subjective and created for the purposes of this article, cyber space does not have any boundaries and they do not exist in a precise way to ensure its security either.

National Institutions

Until 2011, the main government department that was responsible for the informatisation of the country (including the ICT security issues) was the Ministry of the Interior and Administration. After the reorganisation of the government structure in 2011, the Ministry has not only been divided into two new entities, but there was also a split of responsibility for the Polish cyber security. As a result of those changes, the main department that currently looks after the informatisation of the country is the Ministry of Administration and Digitalization. It executes a number of tasks, including those within the scope of public administration informatisation, information technologies, techniques and standards, as well as supporting investments in the IT area, application of the IT solutions in the information society and its development, finally accomplishment of the international commitments of Poland in the informatisation field.[16] On the other hand, the Ministry of Interior is legally responsible for such matters as security and public order protection[17] and, through the Department for State and ICT Registers as well as the Office for the Protection of Classified Information, for the supervision and protection of the ICT systems and networks, and this not only within the Ministry but also in some areas outside it.[18]

The Internal Security Agency is a service that takes care of securing Poland's constitutional order, including the execution of tasks within the scope of the ICT systems security dedicated to process confidential data. The tasks of the Internal Security Agency in this field are effectuated by the Department of ICT Security and specialised divisions.[19] Moreover, also the most important entity operates within the confines of the Department of ICT Security, and it ensures cyber security of public administration entities. It is the Governmental Computer Security Incident Response Team CERT.GOV.PL. "Its chief task is ensuring and developing the capability of public administration units to protect themselves against cyberthreats, in particular against attacks aimed at the infrastructure involving IT systems and networks, the destruction or disturbing of which may considerably threaten the lives and health of people, the existence of national heritage and the environment, or lead to considerable financial losses or disturb the operation of public authorities".[20] CERT.GOV.PL manages the incidents which are protected by the ARAKIS-GOV system, a tool that serves as an early warning system, alerting of Internet threats. The system has been created by CERT-Polska and the Department of ICT Security, and was developed as a result of the need to support the security measures that protect ICT resources of the public administration.[21]

In the majority of countries, one of the most sensitive areas in context of security is the CIP, which also includes the ICT infrastructure systems. Poland is not an exception. According to the currently valid Act of 26 April 2007 on Crisis Management, Article 3, point 2, the definition of CI embraces cybernetic systems that are crucial to the minimal functioning of the economy and the state.[22] The organisation which is relevant to the realisation of the tasks that concern planning and programming of the crisis management and critical infrastructure protection (CIP) is the Government Centre for Security (GCS). The above-mentioned Program emphasises this institution's responsibility for the coordination of the operations concerning the CIIP. In the official declarations related to the planned actions from this field, the GCS notices the necessity to create a favourable environment for the cooperation between the public and private entities. It also announces the launch of a public-private forum which, *inter alia*, will enable the information and knowledge exchange, coordination of the operations with aimed at building a secure CI, including the one related to the ICT sector. This initiative is an interesting attempt to involve private entities in the Polish cyber space protection. GCS is also responsible for the preparation of the "National Critical Infrastructure Protection Programme", the key document from the national security point of view which specifies, *inter alia*, the priorities, objectives, requirements and standards related to the functioning of the CI and the criteria on the basis of which the particular elements of those systems will be determined.[23]

A key role in ensuring cyber security is also provided by the Office of Electronic Communications[24] and the Inspector General for the Protection of Personal Data.[25] Additionally, the Department of Support in Fighting Cybercrimes (pol. Wydział Wsparcia Zwalczania Cyberprzestępczości) operates within the structures of the Bureau of Criminal Investigation of the National Police Headquarters

16 Ministry of Administration and Digitalization, http://mac.gov.pl/spoleczenstwo-cyfrowe/, [access: 29.03.2012].
17 Act on branches of government administration of 4 September 1997, consolidated text.
18 More: Department for State and ICT Registers, http://www.msw.gov.pl/portal/pl/78/6988/Departament_Ewidencji_Panstwowych_i_Teleinformatyki.html, [access: 29.03.2012].
19 Internal Security Agency, *Bezpieczeństwo teleinformatyczne*, http://www.bip.abw.gov.pl/portal/bip/79/154/BEZPIECZENSTWO_TELEINFORMATYCZNE.html, 2012, [access: 29.03.2012].
20 CERT.GOV.PL, *About us*, http://cert.gov.pl/portal/cee/38/77/About_us.html [access: 29.03.2012].
21 CERT.GOV.PL, *System ARAKIS-GOV*, http://cert.gov.pl/portal/cer/4/310/System_ARAKISGOV.html, [access: 29.03.2012].
22 Act on crisis management of 26 April 2007, consolidated text.
23 Government Centre for Security, *National Critical Infrastructure Protection Programme*, http://rcb.gov.pl/eng/?page_id=249, [access: 29.03.2012].
24 Office of Electronic Communications, *Tasks of the President of the Office of Electronic Communications*, http://www.en.uke.gov.pl/ukeen/index.jsp?place=Lead12&news_cat_id=58&news_id=448&layout=7&page=text, [access: 29.03.2012].
25 Inspector General for the Protection of Personal Data, *Responsibilities of the Inspector General for Personal Data Protection*, http://www.giodo.gov.pl/426/j/en/, [access: 29.03.2012].

(pol. Biuro Kryminalne Komendy Głównej Policji). The analysis of *inter alia* international aspects of cyber security falls within the scope of competencies of the Department of Security Policy of the Ministry of Foreign Affairs.

Other Entities

The most important entity responsible mainly for the civil and non-governmental area of the cyber space protection is CERT-Polska. It is a team that was brought into existence to react on cyber security violation cases, and it is functioning in the structures of the Research and Academic Computer Network (NASK). CERT-Polska has been operating since 1996. Its tasks do not differ from standard tasks carried out by other similar organisations. Its main activities include: recording and dealing with incidents that violate cyber security, alarming and informing the users about the existing threats, conducting research and educational activity within the scope of cyber security and raising awareness in this field.[26] CERT-Polska participates in numerous international initiatives, including:[27]

- Forum of Incidents Response and Security Teams.
- HoneySpider Network (HSN) – a joint project between NASK/CERT Polska, Dutch GOVCERT. NL and SURFnet, an academic operator in Holland. The goal is to develop and use the existing and new honeypots, in order to fight the attempts at unauthorised use of systems or information theft.
- Project Worldwide Observatory of Malicious Behaviors and Attack Threats (WOMBAT) – a project aimed at creation of a global monitoring system and analysis of online threats.
- Project SOPAS: Network Attacks Protection System (pol. System Ochrony Przed Atakami Sieciowymi) – realised in consortium by the Military Communication Institute, NASK and ITTI Sp. z o.o., aimed at creation of a prototype system that would protect the federal ICT network.[28]

The project Framework for Information Sharing and Alerting (FISHA), launched in 2009, which set as its main goal the development of the EISAS (European Information Sharing and Alerting System), a pan-European system that includes threat information exchange, deserves major emphasis due to the Hungarian partner. The project has been realised in cooperation with such entities as NASK and the Hungarian CERT (CERT-Hungary), and it has been continued within the confines of the Network for Information Sharing and Alerting (NISHA).[29] Additionally, CERT-Polska is the author of ARAKIS system, which creates an early warning system concerning network threats on the basis of the aggregated and correlated data from various sources.[30] CERT-Polska is not a member of the European Government CERTs group.

Another CERT team that protects the users' security in cyber space in Poland is PIONIER-CERT (it responds to the incidents concerning PIONIER, the Polish Optical Internet: a nationwide broadband optical Network for e-science).[31] It is also worth mentioning the ABUSE-FORUM initiative, an expert group initiated by NASK, which gathers the representatives of CERT teams as well as the teams that ensure the security of Polish ICT operators and the Internet content providers.[32]

National Defence Sphere

Poland belongs to a group of countries that notice the process of the militarisation of cyber space. What is more, this country has begun the process of building its capabilities within the scope of conducting military operations in this field.[33] It results not only from the global tendency heading in this direction, but also from the progressive informatisation of the army and of the entire defence department, which forces the necessity to undertake the actions that will lead to ensuring a higher level of cyber security. Currently, the ICT solutions determine, to a larger and larger extent, the possibilities of the basic functioning of the defence forces, including sending information and data, managing and commanding. Entity that is responsible for cyber security of the Ministry of National Defence (MoND) is the Computer Incident Response System CIRS (pol. System Reagowania na Incydenty Komputerowe).[34] The objective of this system is to ensure the realisation and coordination of the processes of prevention, detection and reaction to computer incidents occurring in the ICT systems and networks of the MoND.[35] The System is supervised by the Director of the Information Technology and Telecommunication Department.[36] Since February 2012, the Director of this Department has performed the role of a Representative of the Minister of National Defence for Cyber Security. The main part of his duties represents supervisory and coordination functions, including participation in preparing annual reports on the state of cyber security. The Representative is supported by the Ministerial Centre for Network Security and ICT Services Management (pol. Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych).[37]

The MIL-CERT team works within the CIRS, and it is a Military Computer Incident Response Team (pol. Wojskowy Zespół Reagowania na Incydenty Komputerowe). The "Strategy of

26 CERT Polska, *O nas*, http://www.cert.pl/o-nas, [access: 29.03.2012].
27 CERT Polska, *Projects*, http://www.cert.pl/projekty/langswitch_lang/en, [access: 29.03.2012].
28 The project assumes an introduction of Sensors, Reaction elements and Decision modules to the autonomous domains, which will enable a cooperation consisting in, among others, exchange of information about the detected threats.
29 A Framework for Information Sharing and Alerting, *The Project*, http://www.fisha-project.eu/the-project, [access: 29.03.2012].
30 CERT Polska, *Projekty*, op. cit.
31 PIONIER-CERT, *Misja*, http://cert.pionier.gov.pl/Misja, [access: 29.03.2012].
32 CERT Polska, http://www.cert.pl/news/tag/abuse-forum, [access: 29.03.2012].
33 J. A. Lewis, K. Timlin, *Cybersecurity and Cyberwarfare. Preliminary Assessment of National Doctrine and Organization*, http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf, Center for Strategic and International Studies, [access: 29.03.2012] , p. 3.
34 *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2012-2022. Projekt*, p. 119.
35 SRNIK, *O SRNIK*, http://www.srnik.wp.mil.pl/pl/2.html, [access: 29.03.2012].
36 Decision of the Minister of National Defence no 357, 29 July 2008, on the organization and operation of the CIRS in the Ministry of National Defence.
37 More: Decision of the Minister of National Defence no 38/Ministry of National Defence, 16 January 2012, on appointing the Representative of the Minister of National Defence for Cyber Security.

Development of the National Security System of the Republic of Poland" anticipates further development of the capabilities of this entity until it will be able to execute technologically advanced functions, including forensic IT and an active response to cyberattacks.[38] The creation of military units dedicated to cyberoperations shows a greater commitment of the country to build its position in the cyber space. Poland has started this process by launching the Cybernetic Security Center in Białobrzegi (pol. Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach) in summer 2010. The aim of the experts in the ICT technologies that work at this Center is to protect the MoND and military command. Also the start of the first "digital battalion", which will have the ability to support soldiers' operations on the battlefield,[39] is being planned. In addition, the strategic documents that describe current situation and the future of the Polish armed forces emphasise further development of the army's possibilities in cyber space. The necessity to create not only the defensive capabilities (including the defence against an electromagnetic pulse attack), but above all, the possibility of offensive operations is being noticed.[40] The most futuristic strategy documents, prepared by military experts, anticipate the creation of the Independent Information Force, which would carry out recognising and electronic fighting methods, psychological actions and operations in the cybernetic environment.[41]

In order to complete the catalogue of the national defence entities, it is necessary to add the Military Counterintelligence Service, responsible for the security of classified information in Poland and which fulfils its duties by means of such initiatives as security accreditation of the ICT systems that process classified information, certification of tools and devices that are related to the ICT security as well as organisation of trainings.[42]

The Polish MoND also develops international cooperation oriented towards enhancing cyber security, especially within NATO. In 2011, the representatives of Poland signed an agreement with the NATO Consultation, Command and Control Agency (NC3A) that facilitates the cooperation within the scope of the development of the defence technology against cyberattacks, intelligence information exchange, reconnaissance and interoperability.[43] In 2010 Poland participated in the NATO Cyber Defence Workshops,[44] and in November 2011 it joined the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[45]

To complete the review of the issues concerning the militarisation of cyber space and involvement of the Polish entities of the national defence in this process, it is worth to mention one more initiative. In September 2011 the President of the Republic of Poland signed the

38 Ibid.

39 W. Lorentz, *Polska na cyberfroncie*, 2010, http://www.rp.pl/artykul/572005.html, [access: 29.03.2012].

40 Ministry of National Defence, *Strategiczny Przegląd Obronny. Profesjonalne Siły Zbrojne RP w nowoczesnym państwie. Raport*, Warszawa 2011, p. 87/89.

41 Ministry of National Defence, *Wizja Sił Zbrojnych RP – 2030*, Warszawa 2008, p. 23.

42 Służba Kontrwywiadu Wojskowego, *Bezpieczeństwo teleinformatyczne*, http://www.skw.gov.pl/ZBIN/bezp_it.htm, [access: 29.03.2012].

43 ALTAIR Air Agency Ltd., *Porozumienie* z NC3A, 2011, http://www.altair.com.pl/start-5874, [access: 29.03.2012].

44 Poland also participated in the European exercises concerning creation of capabilities in the cyber security field – Cyber Europe 2010, organized by the ENISA.

45 J. Sońta, *Przyjęcie Polski do Centrum Cyberobrony NATO w Tallinie*, 2011, http://polska-zbrojna.eu/index.php?option=com_content&view=article&id=14043&Itemid=160, [access: 29.03.2012].

amended Act on Martial Law that allows to declare martial law, state of emergency or state of natural disaster in case of an external threat in cyber space, and which had been proposed as the President's initiative. At the same time, the definition of cyber space has been introduced and it is considered "a space of generating and exchanging the information and which is created by ICT systems".[46] Nevertheless, as the experts rightly notice,[47] the consequences of potential implementation of amended acts require deeper analysis which will demonstrate additional aspects related to cyber security. First and foremost, introduction of a state of exception entails serious effects on the functioning of the society, often limiting its liberties, and at the same time strengthening the controlling possibilities of particular entities. That is why the decision on the implementation of the above-mentioned states of exception must be based on hard facts, verified evidence and well-defined causes. In the case of a cyberattack, however, it is very difficult to specify where the threat is coming from. Moreover, it is not easy to predict if potential outcomes allow to qualify such incident to a catalogue of threats that pose exceptional danger to national security, and which would entitle authorised entities to undertake radical actions which could affect the society.[48] The introduction of the provision on external threat is particularly controversial because the cyber space is a zone beyond geographical boundaries, plus the attacks performed within it can be carried out by an interception of a computer that is situated in different part of the world, which can make it very difficult to prove its "external" character. Therefore, the problem of attribution can have serious consequences. In the face of these reservations, the country should be more eager to enhance the effectiveness of the protection and prevention mechanisms within the scope of cyber security in cooperation with private entities. It should also invest in the technological development which would not only enable it to make preparations against cyberattacks, but also to estimate the threats and to introduce a better adaptation of proper behaviours and reactions.[49]

How Well is Poland Prepared?

On 30 January 2012 the McAfee company together with the Security & Defence Agenda published a report on the resistance level of particular countries to cyberattacks entitled "Cyber-security: the vexed question of global rules". According to the results of the experts' work, Poland is completely unprepared for cyberattacks – on a scale of 1 to 5, it received only 3 points (see figure below).[50] Like every ranking, also this one could become the subject of a discussion and its results could be questioned, even because of subjectivity of the adopted methodology. Nevertheless, the events from the end of January 2012 which took place in Poland unfortunately seem to confirm the diagnosis given by the research. At that time, the hacktivists decided to perform concentrated attacks on the websites of the most important

46 Polish Press Agency, *Stan wojenny w razie zagrożenia w cyberprzestrzeni. Prezydent podpisał ustawę*, http://www.polskatimes.pl/artykul/455144,stan-wojenny-w-razie-zagrozenia-w-cyberprzestrzeni,id,t.html?cookie=1, [access: 29.03.2012].

47 More: Euro-Atlantic Association, 'Instytut Mikromakro' Foundation, *Rekomendacje Zarządu Stowarzyszenia Euro-Atlantyckiego w sprawie wprowadzenia stanu nadzwyczajnego w związku z zagrożeniami z cyberprzestrzeni*.

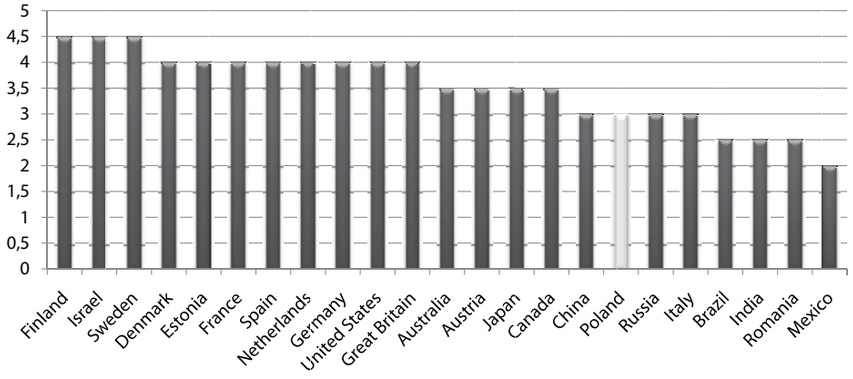
48 Ibid.

49 Ibid.

50 T. Kowalski, *Raport McAfee i SDA: Polskie witryny podatne na cyberataki*, 2012, http://www.wiadomosci24.pl/artykul/raport_mcafee_i_sda_polskie_witryny_podatne_na_cyberataki_224005.html, [access: 29.03.2012].

Polish national administration entities. The attack was a form of a protest against the decision on signing ACTA (Anti-Counterfeiting Trade Agreement). As a result of it, the websites of Sejm, (the lower house of the Polish parliament), Chancellery of the Prime Minister and Ministry of Defence stopped functioning.[51] In addition, the hacktivists also made public the username and password protecting the administrative panel of the Prime Minister's website (username: admin admin, password admin1).[52] If it is true (and everything indicates that it is so), it is not only evidence of a very low level of security measures of the governmental websites, but also a situation that exposes negligence of cyber space protection on the part of the entities which should actually be responsible for that matter. This thesis is additionally enhanced by the statement of the Minister of Administration and Digitalization, who replied to the journalists' question about the entity responsible for this state of the governmental websites protection, that he does not know who administers that network.[53] The website of the Internal Security Agency, which is one of the most important entities that look after Polish cyber security, did not resist the attacks either. What is interesting, since 2009 the Agency prepares audits of the governmental websites protection, calling for the necessity of the improvement of cyber security. In 2010 the Agency's CERT detected 155 attempts at hacking into the governmental websites. During the same year, 93 websites had been examined and 1277 errors had been detected (including 451 serious ones). The data from the 1st, 2nd and 3rd quarter of 2011 indicate that for each 77 tested websites, 740 errors had been detected (including 244 serious ones).[54] Apparently, sometimes even the institutions that have the broadest knowledge about cyberattacks are not capable to resist them.

Fig. 1. SDA and McAfee stress test results. Source: Brigid Grauman, Security & Defense Agenda. *Cyber-security: The vexed question of global rules. An independent report on cyber-preparedness around the world*, 2012. For presentation of test results, a 5-point scale (0-5) was selected, where 5 is the best grade,while 0 is the lowest.



51 TVN24, *"Admin1" chroni dziurawą cybergranicę Polski?*, 2012, http://www.tvn24.pl/1,1732786,druk.html, [access: 29.03.2012].

52 Polskie Radio, *Hasło premiera: admin1. Zobacz najpopularniejsze hasło*, http://www.polskieradio.pl/5/3/Artykul/522756,Haslo-premiera-admin1-Zobacz-najpopularniejsze-hasla, [access: 29.03.2012].

53 T. Kowalski, Minister *Boni nie wie, kto administruje rządowymi stronami, 2012*, http://www.wiadomosci24.pl/artykul/minister_boni_nie_wie_kto_administruje_rzadowymi_stronami_223416.html, [access: 29.03.2012].

54 FORSAL, *W 2010 roku CERT ABW wykrył 155 prób włamań na witryny rządowe*, http://forsal.pl/grafika/587049,89811,porozumienie_acta_rzad_zapomnial_o_cyberbezpieczenstwie.html, [access: 29.03.2012].

The Beginning of the Road

Paradoxically, the biggest weakness of Poland in the field of cyber security is not the lack of a good preparation for cyberattacks. The most important problem is not the fact that in a situation of a real threat the websites of public entities stopped functioning. The cyber space protection is not easy, the possibilities of attacks are unlimited and every day they become more and more sophisticated. Additionally, the success is not announced publicly, we do not hear about a high number of constantly repulsed and foiled attacks in the news. What really is the biggest offence of some entities (also the crucial ones), is the fact that they do not seem to treat this matter with proper seriousness and probably they do not pay enough attention to treat it with, at least, equal importance as the defence from conventional threats.

Apart from the situation related to ACTA that illustrates this problem, an issue concerning the Program, that is the basic document related to the cyber security, is another argument that confirms the above-mentioned statement. The Program, although announced in 2010, is a dead document. Moreover, it should constitute the continuation of the previous Program (for the years 2009-2011), meanwhile, in large part, it is a repetition of the recommendations from the old document. It seems that it is a result of the fact that the implementation of the cyber security steps is being pushed aside or is not executed at all. The decision-makers shift the responsibilities on who should implement essential projects. As a consequence, Poland in reality does not have a functioning cyber space strategy. Therefore, there is a very important postulate to implement the Program and to create the announced "Cyberspace Security Policy of the Republic of Poland".

The attacks from the beginning of the year were not focused on doing any damages, it was a form of protest. Is an actual catastrophe really needed to make the Polish decision-makers treat the issue seriously? Moreover, it is necessary to realise that the incidents that took place due to the signing of ACTA may arouse users' fears and discourage them from making use of the tools that are available within the cyber space. The users' trust is necessary for the informatisation of the society and, as a result, also of the country – a condition that is essential for industrial and economic development.

A singular initiative made by the President, which is applied without reference to more complex operations, is not enough to change the current state of affairs. There is a need for comprehensive system changes, a need to introduce a body that would coordinate the actions of various other entities which have an influence on the cyber security.

A shared responsibility should be monitored. It is necessary to maintain the subsidiary role of the country, but at the same time there is a need to introduce monitoring and evaluation instruments of the implemented operations that improve the security. All of the involved parties, as a result of being fully aware of the importance of the problem, must voluntarily and willingly participate in the cyber space protection. It is essential to build a mutual trust and sense of security which will enable the information and experience exchange. The commitment and collaboration with the public sector is crucial, that is why the cooperation on

the basis of private-public partnerships must be intensified. The state should treat the private sector and scientific circles as important partners. A responsible activity of the decision-makers who will demonstrate their professional attitude by, among other things, consulting the most important documents with the experts, should be the catalyst of this process. It is also worth to consider the establishment of an advisory body that would include experts from the three sectors and which could serve as support to the entity coordinating the operations related to the cyber space. Moreover, education and an increase in the awareness should be realised among the society and the elites.

No less important is the collaboration with external entities. The cooperation with international partners (countries or organisations) on the basis of multilateral agreements and bilateral projects is essential for building a secure cyber space. The Council of Europe Convention on Cybercrime should be ratified as soon as possible.

Polish non-governmental entities, private ones and the military sector seem to have a better understanding of the necessity to protect cyber space. The actually undertaken initiatives, projects or international cooperation are signs of it. The rest of the crucial players responsible for the national security should also follow this path.

5. Cyber Security in Slovakia

Jozef Vyskoč

Relevant Bodies

Let us start with an observation that no state-sponsored institution in Slovakia is specialised exclusively in the whole spectrum of cyber security issues. Instead, various state institutions, as well as other organisations, address partial topics related to cyber security. In general, the National Security Authority (NSA) takes care for classified information, while the Ministry of Finance (MoF) addresses the rest, however, some specific topics are supervised by the Ministry of Interior (MoI), Ministry of Defense (MoD), Personal Data Protection Office (PDPO) and Slovak National Accreditation Service (SNAS). Besides that, there are some professional communities, as well as nongovernmental organisations (NGOs), whose activities, to certain extent, address specific cyber security-related aspects.

State Institutions

The NSA serves as an official authoritative body for protection of classified information, encryption services and electronic signature. Its roles include, among others:

- issuing security clearances for handling classified information (for physical persons as well as for corporate entities),
- certification body for technical safeguarding devices and for secure devices for electronic signatures,
- Central encryption office,
- Root certification authority and accreditation of certifications authorities,
- Central Registry for exchanged foreign classified information.

The NSA is also national authority for cyberdefence and in this role is responsible for intersectoral working group established to coordinate NATO-related cyberdefence activities in Slovakia.

Building of information society belongs to areas supervised by MoF, thus naturally it is in charge of security of non-classified systems (information security issues). This is accomplished by the Division of Legislation, Standards and Security of Information Systems (within the Information Society Section). Its main tasks include:

- responsibility for critical infrastructure protection in the sector of information and communication technologies,
- preparation of strategic documents, standards, proposals, opinions and other documents for information systems of public administration (ISPA) and their security,
- observe, analyze and evaluate the state of security of ISPA,
- represents SR in EU bodies and institutions for information security.

Here also belongs the Committee for Information Security as an advisory body composed of representatives of MoF, MoI, NSA, SNAS, PDPO, Governmental Office, Slovak association for information security, IT Association of Slovakia, Commenius University and an independent expert serving also as a liaison officer for ENISA. It should be noted, however, that publicly available information suggests that the last meeting of the Committee for Information Security was in March 2008.

MoF in its structures also manages the Computer Security Incident Response Team (CSIRT.SK) whose core tasks include:

- response to the information security incidents in the SR in cooperation with the owners and providers of impacted parts of the national critical infrastructure, telecommunication operators, ISPs and other public bodies (police, investigators, courts),
- raising awareness in the field of information security,
- cooperation with foreign counterparts and organisations and representation of the SR in the field of information security internationally.

CSIRT.SK, in its role of a national CSIRT, is tasked to provide services mainly for government in order to promote responses against IT security incidents aimed at national critical infrastructure as well as services for public administration (excluding classified information and military incidents). As of now, services for public are rather restricted, their expansion in the future is planned.

MoI (through its Section of Civic defence) is assigned tasks related to preparation of strategic documents and conceptions, and coordination and control in the areas of crisis management and critical infrastructure protection. In the structures of Police Corps there is also the Institute of Forensic Science, whose Department of Data Analysis deals with forensic investigations of computer and communication systems and provides expert witnesses for the area of computer crime.

MoD provides expert representation of Slovakia in the NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE) in Tallinn, Estonia.

Though personal data protection seems to be a rather specialised task within the whole cyber security area, its inclusion here is justified by the fact that the current Data Protection Act and PDPO as respective supervisor urges organisations to dedicate more effort to security of their systems (the urge is backed by a possibility to impose a fine if the effort is not sufficient). Particularly, in addition to general obligation to protect data in specific cases it also explictly requires organisations to perform security analysis and to put together security project. Consequently, it contributes to general awareness of the need for security and of security principles and best practices. Moreover, the role of the PDPO is important on its own as it provides the necessary feedback to ensure better balance between security measures proposed by the state administration (e.g. against terrorism) and preservation of citizens' right for privacy.

Though not obligatory, organisations may choose to improve their security by implementing the so called Information Security Management System (ISMS) as defined by the standard ISO 27001. SNAS thus participates in the cyber security-related activities indirectly, by accreditation of certification bodies performing certification of conformance to the ISO 27001 standard. It should be noted, however, that SNAS expertise lies in the area of conformity evaluating principles and procedures and to evaluate security-related aspects it makes use of external experts. As of now 12 certification bodies (including some foreign ones) are accredited to provide certification of conformance to the ISO 27001 standard in Slovakia.

Other Entities

Some NGOs, especially those focused on the area of security and defence policy, also work towards including cyber security issues in their activities. Particularly, Centre for European and North Atlantic Affairs (CENAA) strives for inclusion of papers on cyber security issues in its annualy published collection of papers "PANORAMA of global security environment" (international team of authors, edited in cooperation with MoD). Slovak Atlantic Commision (SAC) made cyberterrorism the main theme of No. 4/2008 of their magazine Euro-Atlantic Quarterly, included cyber security into the topics of the distinguished annual GLOBSEC conference it organises, and also participates in preparation of this document. Euro-Atlantic Center (EAC) included a conference titled "Information security in the Slovak Republic" in the third cycle of its project "National Security Table". It should be noted, however, that as of now these NGOs, in their cyber security-related activities, make use of external experts as they do not have sufficient internal expertise (yet).

There are two professional communities explicitly focused on information security or some related specific area, namely Slovak association for information security (SASIB) and Slovak chapter of the international Information Systems Audit and Control Association (ISACA Slovensko). Visible activity of SASIB consists of annual organisation of the conference "Information security" of rather local character (speakers are members of SASIB). ISACA Slovensko is more active – two annual conferences (with Slovak as well as foreign speakers), various seminars and more informal "evening club meetings". Cyber security is also among the activities of the Slovak chapter of the Armed Forces Communication and Electronics

Association International (AFCEA Slovak Chapter). More generally oriented Slovak Society for Computer Science (SSCS) has one of its several special interest groups dedicated to information security issues, its activities are rather invisible, though. Most activities of these professional communities are primarily intended mainly for their members.

In addition to that, some less formal civic groups are also devoted to some specific security-related topics, as e.g. European Information Society Institute (focusing on rights and freedoms of Internet users and service providers) or Progressbar – the first hackerspace in Slovakia with quite a lot of security-related activities, mainly of technical nature.

Key relevant Legislation

- Act No. 215/2002 Coll. on electronic signature and on the amendment and supplementing of certain acts as amended by Act No. 679/2004 Coll., Act No. 25/2006 Coll., Act No. 275/2006 Coll. And Act No. 214/2008 Coll.
- Act No. 428/2002 Coll. on protection of personal data, as amended by the Act No. 602/2003 Coll., Act No. 576/2004 Coll., Act No. 90/2005 Coll. and Act No. 583/2008 Coll.
- Act No. 215/2004 Coll. on protection of classified materials and on amendment to certain laws as amended by Act No. 638/2005 Coll., Act No. 255/2006 Coll., Act No. 330/2007 Coll., Act No. 668/2007 Coll., Act No. 291/2009 Coll., Act No. 400/2009 Coll., and Act No.192/2011 Coll.
- Act No. 275/2006 Coll. on information systems in public administration as amended by Act No. 678/2006 Coll., Act No. 553/2008 Coll., Act. No. 570/2009 Coll.
- Regulation of Ministry of Finance No. 312/2010 Coll. on standards for information systems in public administration (includes security standards for ISPA).
- Act No. 45/2011 Coll. on critical infrastructure.
- Act. No. 351/2011 Coll. on electronic communications.

The so called Act on Information Security is under preparation and only its preliminary design has been published. It appears that the act is planned to be really ambitious and complex. According to the published preliminary design one can expect that the act will:

- introduce a special classification scheme for ISPA together with minimal security requirements for each classification level,
- define role and tasks assigned to specialised incident-response units (like CSIRT.SK),
- deal with standardisation in the area of information security,
- create education and certification framework and define minimal knowledge level for those with information security management competencies,
- define the role of the security in eGovernment (including secure communication or identification and authentication in relation to eGovernment services),
- determine priorities for critical ISPA and framework for coordinated response in the case of large-scale cyber space incident,
- create general framework and conditions for use of specialised security technologies, like RFID, biometrics, voice recognition, etc.,
- define minimum process and organisational aspects for management of information security – explicitly for public administration, but it is envisaged that it could serve as a voluntary reference framework for private sector as well,
- define requirements and rights for inspections of security requirements fulfilment and possible sanctions,
- establish framework for mandatory notifications in the case of serious security breaches.

As of now, it is not known whether and when the complete text of the act will be prepared and published for discussion, and to what extent the preliminary design be reflected – the preliminary design has been approved in February 2010 and changes in the ICT as well as new concepts might render it inadequate for the future.

Relevant Documents

The main document covering the information security in the SR is "the National Strategy for Information Security", approved by the Slovak Government on August 27, 2008. The document defines three strategic goals:

1. prevention – to protect Slovak digital space to prevent occurrence of security incidents,
2. readiness – to be able to effectively react in the case of security incidents, minimise their impact and time needed for recovery,
3. sustainability – to achieve, sustain and expand competences of the Slovak Republic in the area of information security,

and seven strategic priorities:

1. protection of human rights and freedoms in connection with using national information and communication infrastructure,
2. building of awareness and competences in information security,
3. creation of secure environment,
4. increase efficiency of information security management,
5. ensuring adequate protection of state information and communication infrastructure, including information and communication infrastructure supporting critical infrastructure,
6. national and international cooperation,
7. expanding national competence,

and provides an outline of subsequent activities necessary to achieve stated goals. It is remarkable that the Strategy itself declared that it has been formulated for five years term (2008-2013) only.

From the steps envisaged by the Strategy as of now only few subsequent documents were created – Action Plan, "Concept of Information Security Education" and documents necessary for creation of CSIRT.SK.

"Concept of Information Security Education", approved in May 2009, has aspirations to include information security into the primary and secondary schools. It assumes that the content of the

education is based on a watered-down version of the so called Common Body of Knowledge (CBK), normally used in certification of security professionals (Certified Information System Security Professional – CISSP).

As for the Act on Information Security, announced in the Strategy, only preliminary design has been prepared and published. Besides creation of these documents and CSIRT.SK no subsequent steps or activities with real consequences formulated in the Strategy are known.

International Cooperation

International cooperation in the cyber security area exists on two levels – state sponsored and other, including private sector, NGOs or even interested individuals. State bodies like NSA, MoF, MoI, PDPO and CSIRT.SK represent Slovakia in the respective international organisations (usually within the EU or NATO structures). There is no complete information on participation of private organisations, NGOs or individuals in international cooperation available, though such cooperation clearly exists in various forms like participation in research projects, speakers on conferences, memberships in specialised international working groups, etc. These two levels of cooperation run in parallel and independent of each other, though sometimes may complement themselves. Let us take cooperation with the NATO CCDCoE as an example – while MoD as a state body provides expert representation of the SR in the Centre, independently of that there exists also civil individual cooperation in the form of membership in the Program Committees of the annual CyCon conferences organised by the CCDCoE.

It is worth to mention that the SR signed the Budapest convention on cybercrime in 2005 and ratified the document in 2008.

Other Relevant Activities

MoD cyberdefence specialists in 2010, 2011 and 2012 actively participated in the NATO Cyber Defence Exercises (NATO CDX).

In 2011 CSIRT.SK together with MoF organized the first national exercise on critical information infrastructure protection – Slovak Information Security Exercise 2011 (SISE 2011). Besides MoF and CSIRT.SK also MoI, Government Office of the SR, Telecommunications Regulatory Authority of the SR and DataCentrum, as well as Computer Emergency Response Team Austria (CERT.at) and Computer Security Incident Response Team Czech Republic (CSIRT.CZ) participated. In addition to that, MoD and CESNET Computer Security Incident Response Team were involved as observers.

Analysis and Conclusions

At the first sight, it appears that Slovakia has a fair amount of coverage of cyber security-related issues – several state bodies are assigned respective roles, there exists basic legislation and even "The National Strategy for Information Security". The problem, however, is that the mere existence of bodies or documents is not sufficient if even a brief peek at the inside reveals serious defects. For example, one could note that in the area of cyber security, state interests and citizens' interests are nowhere explicitly and adequately identified and also are not reflected in the declared priorities. The consequences of such fault can be demonstrated in practice by implementation of one of the eGovernment services – to use it one had to "correctly configure" a computer, where the "correct configuration" actually meant a substantial degradation of the standard (medium) security level of the used browser. Clearly justifiable interests of citizens/users of the service were ignored in this case – and what is worse, an analysis of relevant documents (like Strategy or regulation on security standards for ISPA) shows that there is nothing there to prevent reappearance of such approach.

Let us start our analysis with an observation that the notion of cyber security/information security can be treated and understood on various levels of abstraction – from a collection of purely technical threats and corresponding technical measures implemented on a particular system or device up to formulation of state positions for international negotiations concerning cyber space. Another viewpoints differentiate between the short-term and long-term thinking and measures, or between ensuring operation security of a system and more complex view on security for the whole lifecycle of a system starting from its design. Also looking at the history of the discipline shows how its character developed – from original understanding of computer security as a problem solvable by application of hardware and software measures until today's view of complex problem with solutions drawing from a mix of mostly nontechnical disciplines like psychology, sociology, economy or management (while technical measures are included as well, their role is not seen as dominant).

Now let us take a closer look at the key document – "the National Strategy for Information Security". Though this document is supposed to be of strategic character, this is not the case, as e.g.:

- key "players" and their interests and possible conflicts are not properly identified (owners and IS users are not the only players, as there are also suppliers of IS and relevant basic infrastructures, providers of various services or important decision-makers whose decisions may have significant effect on cyberdefence effort; also citizens, whose personal data is stored and processed in various IS, have their rights and interests that need to be respected),
- it focuses mainly on operation security and technical security issues, completely ignoring important phases of the design, implementation and testing of the IS and the need to respect security requirements there,
- apparently it considers only "classical" types of systems and completely ignores new trends like cloud computing, BYOD ("bring your own device"), or Internet of Things; moreover there is not even a mention of a need to keep pace with the changes in ICT, cyber security, requirements and needs, etc.,
- document represents short-term thinking, as illustrated e.g. by the absence of a reference to the need to provide analysis of trends in cyber security, qualified predictions and support for subsequent strategic planning,
- only "low-level" international cooperation is considered (namely incident handling, standardisation and possibly research), the need for providing qualified support for

"high-level" international negotiations on topics related to, or including cyber security issues is not even mentioned.

Proposals presented in the subsequent "Concept of Information Security Education" are also debatable, as the idea to use the CBK, originally aimed at *security professionals*, in general education (especially on the level of primary and secondary schools) seems to be rather unrealistic, even if the watered-down CBK is considered. Moreover, once again the effort is concentrated on mostly technical threats and measures.

Also state institutions addressing cyber security issues seem to be preoccupied with operation security issues and/or questions of jurisdiction – lack of forward-looking thinking on more abstract cyber security issues is visible even for the supposed advisory board (Committee for Information Security). Professional societies direct their activities mostly towards their members and generally avoid contemplation on more abstract cyber security issues. On the other hand, such more abstract views seem to attract NGOs, however, till now their activities were mostly focused on awareness raising, not to provide visions, constructive comments or recommendations (hopefully this document represents the first step to change that).

The sad fact is the lack of objective data available to estimate how secure or vulnerable is Slovak cyber space, thus we provide just some (nontechnical and subjective) observations here. Social networks are quite popular in Slovakia, providing a platform for fast and successful spreading of disinformation as demonstrated before Census 2011 official start. Also, there were some cases of hacktivism, but till now actions performed and their impacts were rather mild. What is important, though, is that the state bodies apparently do not pay attention to such threats as demonstrated by the lack of proper (fast and qualified) response to such out-of-the-ordinary events.

Having this in mind, our main conclusion is that understanding and treatment of cyber security issues in Slovakia are not yet fully developed as most of institutions and activities are focused on operation security of ICT systems and distribution of jurisdiction only. Also, though there are visible activities in the area of cyberdefence in Slovakia, these are rather low-level oriented (technical measures, preparation of specialists, etc.). High-level cyberdefence activities, including proper education/training of decision makers on the state level and their connection with executive cyberdefence formations, are missing.

6. Cyber Security in Hungary

Joanna Świątkowska

Cyber Security – Foundation of Hungary's Security?

The key documents dedicated to the national security of Hungary, which set its main goals and define its major challenges, recognise the changes in the trends of the contemporary threats, including the expansion of risks related to cyber security. As early as on 31 March 2004, when the previous "National Security Strategy of the Republic of Hungary" was adopted, the development of the information and communication technologies (ICT) was seen as a process that had been bringing along new threats that changed the international relations and national security.[1] On the one hand, the strategy emphasised the necessity of further development of the Hungarian information society and recognised the advantages which result from that process. On the other hand, the authors of the document accentuated the challenges that are a consequence of the country's informatisation. The vulnerabilities of the ICT networks and systems include their overloading, spreading of viruses, disinformation, possibility of intrusion and information theft, posing in this way many threats which are seen as serious risks to national security.[2]

The necessity of developing a modern and secure infrastructure of governmental information systems was identified as a primary measure in the area of building cyber security. Additionally, it was noticed that coping with the security challenges required close cooperation with Hungary's allies, as well as ICT service providers and research centres.[3] It is worth noticing that the need for public-private cooperation was also included in this fundamental document related to security.

The 2004 "National Security Strategy of the Republic of Hungary" stayed in force for eight years. In February 2012, the Hungarian government has adopted a new "National Security Strategy".[4] Since the previous strategy was introduced, the use of the Internet in Hungary has strongly expanded. The percentages of regular and frequent Internet users as well as the use of a number of Internet services are more or less equal to the EU averages.[5] Processes like informatisation have brought a shift

1 *The National Security Strategy of the Republic of Hungary*, http://www.mfa.gov.hu/NR/rdonlyres/61FB6933-AE67-47F8-BDD3-ECB1D9ADA7A1/0/national_security_strategy.pdf, [access: 17.03.2012].
2 Ibid.
3 Ibid.
4 MTI, *Hungary adopts national security strategy, 2012*, http://www.politics.hu/20120222/hungary-adopts-national-security-strategy/, [access: 17.03.2012].
5 *Scoreboard: Hungary*, http://ec.europa.eu/information_society/digital-agenda/scoreboard/countries/hu/index_en.htmhttp://ec.europa.eu/information_society/digital-agenda/scoreboard/countries/hu/index_en.htm, [access: 17.03.2012].

in the perception of Hungarian safety. Those changes have been reflected in the new strategy, which strongly focuses on unconventional threats, stating that "the risk of an attack against Hungary or its allies with traditional arms is negligible."[6] Among all the unconventional challenges, cyberthreats clearly stand out. The document predicts that the number of cyberattacks will multiply in the nearest future and they will become a burning problem, which makes the need for cyberprotection even more urgent. The document recommends that "systems should be strengthened in conjunction with the country's alliance partners, especially those within the EU."[7] The emphasis put on the international cooperation opens up possibilities for cooperation also within the Visegrad Group (V4).

Hungary belongs to a group of countries where mainly civilian agencies are in charge of ensuring cyber security, and where the discussion on the militarisation of cyber space is not very advanced. Researchers from the Center for Strategic and International Studies name the approach to cyber security as "traditional" and indicate that this attitude usually comes along with "assigning responsibility to science ministries and creating specialised units within the national police."[8] Despite the fact that the main actor responsible for the Hungarian cyberdefence system is, indeed, a civilian organisation (the National Cyber Security Center), below there are introduced the most important public entities involved in the process of ensuring cyber security.

Overview of Main Actors

The widespread use of the ICT is treated as an essential part of Hungary's development. Therefore, the decision-makers try to build a common trust to the ICT tools and to recognise cyber security as an area of governmental responsibility and intervention.[9] In 2011, the European Network and Information Security Agency (ENISA) prepared an individual country report on the Network and Information Security (NIS) of each member state.[10] In the part devoted to the national authorities' responsibilities related to the NIS, the document enumerated, *inter alia*, the following entities:

- MEH EKK (Prime Minister's Office, Electronic Government Centre) – responsible for the implementation of e-Government and the supervision of IT development;
- Ministry of Transport, Telecommunications, Energy – responsible for further development of the ICT sector;
- National Media and Infocommunications Authority – responsible for the undisturbed operation, in compliance with pertaining legislation in force, of the media and the markets for electronic communications, postal and information technology services;
- National Bureau of Investigation – a cybercrime division of the Hungarian police;
- Data Protection Commissioner of Hungary – national supervision over the lawfulness of processing personal data, keeping databases, etc.;
- Parliamentary Informatics Commission – responsible for information policy development;
- Ministry of Defence – responsible for national security, including the security of information;
- Ministry of Justice and Law Enforcement – responsible for crime prevention and data protection.

6 MTI, *Hungary adopts national…*, op. cit.
7 Ibid.
8 J. A. Lewis, K. Timlin, *Cybersecurity and Cyberwarfare 2011*, http://www.unidir.ch/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf, Center for Strategic and International Studies, p. 3, [access: 17.03.2012].
9 E. M. Brunner, M. Suter, *International CIIP Handbook 2008/2009*, Center for Security Studies, p. 182.
10 The European Network and Information Security Agency, *Hungary Country Report*, 2011, http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Hungary.pdf, p. 25 [access: 17.03.2012].

Since the report was released, the structure of the Hungarian government has significantly changed. Modifications also caused the reorganisation of the competences in the field of cyber security. The most important changes included closure of the Electronic Government Centre as well as the Ministry of Transport, Telecommunications and Energy. Currently, the Ministry of National Development has become responsible for the tasks related to the infocommunications, including ensuring the viability of information technology and public administration IT infrastructure, tasks related to electronic media, frequency regulation, information society and postal affairs. As part of the government reorganisations, since 12 September 2011 the Deputy of the State Secretariat for Infocommunication (Zsolt Nyitrai) discontinued his work. Vilmos Vályi-Nagy remained the Deputy State Secretary for Government Information Technology and the unit under his supervision will be directly subject to the Minister.[11]

It is said that changes in the Hungarian government result from the need for an efficient management of the consequences of the economic crisis. The changes in the government structure, according to official statements, are dictated by the necessity to reduce bureaucracy and state costs and to pursue greater transparency.[12] Closure of the office of State Secretary for Infocommunication may be seen as controversial, especially after the period of the Hungarian presidency of the Council of the European Union, when this resort was very active and successfully focused public attention on essential cyber security matters. Moreover, it was an entity that coordinated the activities associated with informatisation.

The above-mentioned decisions are not the only puzzling ones made by the Hungarian government. The "Hungarian National Security Strategy" emphasises that catching up with the ICT standards of the developed world is an important task for Hungary.[13] This priority is supposed to have an indirect positive impact on Hungary's economy, social life and ability to assert its interests. Meanwhile, the Hungarian government has implemented actions which are contradictory to that commitment. In October 2010, a new "crisis tax" was introduced. The tax applies to several parts of the Hungarian economy, including telecommunications services. This decision made the European Commission open law infringement proceedings in March 2011.[14] Additionally, in December 2010 the new Media Act was adopted. The act opened the possibility of delaying the analogue TV switch off under certain conditions until 31 December 2014.[15]

Another controversial modification in the structure of the Hungarian government which affects the cyber space is a change that came into force with the new Hungarian Constitution. The new Constitution "established the National Agency for Data Protection to replace the former Data Protection Commissioner's Office, prematurely ending the six-year term of the Data Protection Commissioner with no interim measures put in place"; in addition, "the new rules allow the Prime Minister and the President to appoint or dismiss any new supervisor on arbitrary grounds."[16]

11 Ministry of National Development, *Changes in the internal organisation of the Ministry of National Development as from 12 September 2011*, http://www.kormany.hu/en/ministry-of-national-development/news/changes-in-the-internal-organisation-of-the-ministry-of-national-development-as-from-12-september-2011, [access: 17.03.2012].
12 Ibid.
13 *The National Security Strategy…*, op. cit.
14 *Scoreboard: Hungary*, op. cit.
15 Ibid.
16 J. Baker, *EU warns Hungary over weak data protection law*, http://www.computerworlduk.com/news/public-sector/3330681/eu-warns-hungary-over-weak-data-protection-law/, 2012, [access: 17.03.2012].

The independence of the entity responsible for data protection is guaranteed by the EU (Article 16 of the Treaty on the Functioning of the EU, Data Protection Directive). Due to controversial decisions of the Hungarian government in this field, the European Commission has launched law infringement measures against it.[17]

CERT – Hungary and Critical Information Infrastructure Protection

The ICT systems are treated as a part of the critical infrastructure (CI); destruction of their interoperability can damage national security, citizens' lives and assets or the proper functioning of the Hungarian economy or public services.[18] Therefore, it is said that protection of those ICT elements must be treated with an exceptional commitment. In December 2007, the National Security Cabinet of the Government decided to found an Information Security Inspectorate and a coordination body for the security of critical information infrastructure (CII).[19]

One of the most important institutions on the map of the entities that are responsible for cyber security, especially for the Hungarian CII protection (CIIP), is CERT–Hungary, operating within the Theodore Puskas Foundation since January 2005 on the basis of a public service agreement. In January 2010, CERT-Hungary was renamed as the National Cybersecurity Center (NCC) by the Government Decree. The Center was created "to protect the Hungarian CII and the security of the communication through the central governmental system, as well as to mitigate the consequences of virus and other attacks."[20] Additionally, the Center represents Hungary in international cooperation and organisations specialised in cyber security and protection of critical information infrastructure (including FIRST, TF-CSIRT TI, Meridian Process, IWWN, APWG).[21] Finally, the NCC is also a member of European Government CERTs group.[22]

This organisation also participates in the preparation of strategies and regulations related to information and network security as well as CIIP. The work of CERT-Hungary is supervised by the Prime Minister's Office. The tasks of the organisation include:[23]

- coordinating responses and countermeasures to serious IT security breaches against government networks and critical information infrastructures;
- promoting information exchange with the critical sectors;
- coordinating with national and international counterparts to enhance national readiness measures;
- acting as the national contact point for international CSIRT and CIIP organisations;
- raising awareness in the field of information and network security. The Centre cooperates with Hungarian law enforcement organisations as well as academic and industrial representatives involved in cyber security.

17 Ibid.
18 Brunner, Suter, *International CIIP…*, op. cit., p. 180.
19 Ibid., p. 181.
20 *Hungarian Government Decree No. 223 of the year 2009 on the security of electronic public service*, Article 8, published in the Official Gazette on October 14th.
21 CERT-Hungary, *About us*, http://www.cert-hungary.hu/en/node/6, [access: 17.03.2012].
22 *European Government CERTs (EGC) Group*, http://www.egc-group.org/, [access: 17.03.2012].
23 CERT-Hungary, *About us*, op. cit.

The NCC coordinates a Supervisory Control and Data Acquisition (SCADA) working group, which is jointly organised by government agencies and the operators of SCADA networks, which is a very interesting example of public-private cooperation.[24] The NCC is active in the field of international cooperation – it has launched several interesting initiatives in the recent years. One of them was a meeting with Chinese delegation in 2007 aimed at building better cooperation and closer relations between government network security centres of the two countries.[25] In March 2012, a similar official visit took place, this time made by CERT-RO, the Romanian national CERT. The visit resulted in mutual familiarisation with the countries' technical capabilities and preparation of a protocol for information exchange.[26]

In context of the subject matter of this publication, it is particularly worth to underline the bilateral cooperation between Hungary and Slovakia. The cooperation has begun at the end of 2005, when CERT-Hungary was asked to assist in the creation of the Slovakian governmental CERT. Later in 2010, the Slovakian GovCERT, CSIRT.SK, visited the NCC with the goal to start cooperation aimed at supporting CSIRT.SK on its road to membership in international CSIRT forums and at deepening the partnership between those two cyber security centres.[27]

Interestingly, the cooperation started during the "Visegrád Workshop", an event which was devoted to international cooperation and communication on critical infrastructure protection between Poland, Slovakia, Hungary, Austria, Slovenia and the Czech Republic. The "Visegrád Workshops", as well as the bilateral experience of the Slovak-Hungarian partnership, should be used as an inspiration for deeper cooperation in the field of cyber security in Central and Eastern Europe, especially in the V4 Group.

There are also other kinds of CERT organisations in Hungary, namely:

- Hun-CERT – it is operated by the Computer and Automation Research Institute of the Hungarian Academy of Sciences (MTA SZAKI) and sponsored by the Council of Hungarian Internet Service Providers (ISZT). Hun-CERT serves mainly the interests of the members of the council. Additionally, the institution distributes information relevant in terms of network security among the general public.[28]
- The NIIF-CSIRT (Computer Security Incidents Response Team of the National Information Infrastructure Development Program) – its aim is to help the members of the academic networks (NIIF and HUNGARNET) to cope with cyber incidents which pose a threat to their security by dissemination of warnings and security-related information.[29]

Hungarian Presidency in Service of Cyber Security

Cyber security was chosen as one of the priorities of the Hungarian Presidency in 2011. During that period, Hungary organised several sponsored workshops and conferences. One of them was an international expert conference entitled "Cyber Security: Challenges and Policies", which took place in Budapest on 2nd May 2011 and was hosted by the Hungarian Ministry of Defence. The main topic of this

24 Brunner, Suter, *International CIIP…*, op. cit., p. 187.
25 CERT-Hungary, *Chinese Delegation at CERT-Hungary*, http://www.cert-hungary.hu/en/archive/200708, 2007, [access: 17.03.2012].
26 CERT-Hungary, *Hungarian-Romanian CERT cooperation*, http://www.cert-hungary.hu/en/archive/201203, 2012, [access: 17.03.2012].
27 CERT-Hungary, *Slovakian Governmental CERT visits CERT-Hungary*, http://www.cert-hungary.hu/en/archive/201006, 2010, [access: 17.03.2012].
28 Brunner, Suter, *International CIIP…*, op. cit., p. 187.
29 Ibid.

event was the cyber space as a potential "theatre of war", and its goal was to work on the international community's response to this potential threat. The most important conclusions stated that the international community is not prepared for militarisation of cyber space. Appropriate legislation is missing and "there is no generally accepted Internet 'code of conduct'".[30] While looking for an answer to those challenges, the participants of the conference recommended, among other things, extensive international cooperation which should lead to development of a broad consensus on the permitted actions in the cyber space. Moreover, a technologically advanced response to cyberthreats, constant improvement of the professionals' qualifications and sharing the knowledge and experiences are highly recommended. The cooperation between NATO and the EU was strongly emphasised.[31]

The aim of another event which took place during the Hungarian Presidency, the Telecom Ministerial Conference, was to discuss the importance of CIIP. During the conference, a crucial need for cooperation in that field was underlined, with a special emphasis put on the call for communication and exchange of information between the ministers of Member States. Additionally, the participants recommended to improve the situation through the adoption of the Council's conclusions.[32] The conference was preceded by a meeting of the representatives of the EU-US Justice and Home Affairs in Gödöllo (Hungary), during which the participants reaffirmed "their shared commitment to deepening cooperation" in terms of cyber security and defined "the issues to be tackled by the EU-US Working Group on Cyber-Security and Cyber-Crime".[33]

One of the most important Hungarian Presidency achievements was the actual progress in the works towards the advancement of the ENISA's operation. What is worth noticing is that, during that period, the draft regulation, which extended the Agency's mandate for the next 18 months with intact powers of this organisation, was generally approved.[34] Moreover, the Hungarian Presidency was able to achieve a theoretical agreement on the responsibilities of the Agency and of its bodies.[35]

Interesting Facts and Initiatives

Hungary seems to recognise the process of militarization of cyber space and is gradually engaging in various international initiatives that work on cyberdefence. On 23 June 2010, Hungary became a sponsoring nation of the NATO Cooperative Cyber Defence Centre of Excellence, which is dedicated to cyber security. According to the official statement, "the Hungarian staff officer was assigned to work within the Training and Doctrine Branch".[36] Additionally, Hungary has been invited to enter the NATO's E-crime Defence Task Force, a formation which aims at fighting "cybercrime and cyberterrorism in the international arena." The fact of joining the E-crime Defence Task Force

30 Á. Draveczki, *Cyberspace could also be war theatre*, http://www.eu2011.hu/news/cyberspace-could-also-be-war-theatre, 2011, [access: 17.03.2012].

31 Ibid.

32 Ministry of National Development, *European network security and action against global cybercrime on the agenda*, http://www.kormany.hu/en/ministry-of-national-development/news/european-network-security-and-action-against-global-cybercrime-on-the-agenda, 2011, [access: 17.03.2012].

33 *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats*, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246, 2011, [access: 17.03.2012].

34 Ministry of National Development, *Handover between the Hungarian and the Polish Presidency Telecommunications and Information Society Dossiers*, http://www.kormany.hu/en/ministry-of-national-development/news/handover-between-the-hungarian-and-the-polish-presidency-telecommunications-and-information-society-dossiers, 2011, [access: 17.03.2012].

35 The European Network and Information Security Agency, *Agency Mandate prolonged by the Council*, http://www.enisa.europa.eu/media/news-items/agency-mandate-prolonged-by-the-council, 2011, [access: 17.03.2012].

36 NATO Cooperative Cyber Defence Centre of Excellence, *Hungary joins the Centre*, http://www.ccdcoe.org/188.html, 2010, [access: 17.03.2012].

coincided with a new initiative of the Hungarian government, intended to battle cybercrime. The government decided to provide training classes at the Zrinyi Defence Academy, where graduates will be trained to be able to fight international cybercrime. This initiative has to be seen as a step towards enhancing human factor in the fight against cyberthreats. Time for this decision seems to be right due to the fact that the media recently reported that a group of Hungarian student hackers succeeded in breaking the defence networks.[37]

As a Member State of the EU, Hungary took part in the pan-European exercise on CIIP called Cyber Europe 2010, organised by the EU Member States and supported by the ENISA and the EU's Joint Research Centre. Participants in Cyber Europe 2010 were only representatives of the public sector from the EU member states, including ministries, national regulatory agencies, organisations responsible for CIIP and CSIRTs. Hungary was represented by CERT Hungary. According to the report, "this experience has shown that even at the national level, Hungary is needed to do plenty of information security incident management, critical information infrastructures security coordination at the government level (…)".[38] Hungary organises its own cyber exercises, aimed at improving its preparedness and ability to recover from the potential threats. The national exercises are conducted regularly (at least every third year) and involve all entities from the telecommunications sector. Furthermore, more often small exercises also take place, and also other sectors (energy, oil, gas, etc.) are involved in those events. This allows to provide profiled tools and measures aimed at recovery.[39]

The Convention on Cybercrime is the first international treaty adopted by the Committee of Ministers of the Council of Europe on 8 November 2001, which deals with computer and Internet crimes. The purpose of this innovative document is to harmonise national laws, advance investigative techniques and improve international cooperation. The Convention is also known as the Budapest Convention and it was signed by Hungary on 23 November 2001. Then, it was ratified on 4 December 2003 and came into force on 1 July 2004.[40]

Apart from that, Hungary has an interesting scheme for security evaluation and certification. A special institution – Hungarian Information security Evaluation and Certification Scheme (MIBEST) works in a field of testing the software security. Additionally, the government launched an Information Security Management Framework (MIBIK), which evaluates security actions at an organisational level.[41]

To end this section dedicated to some interesting aspects of Hungarian cyber security, it is worth mentioning the Hungarian Financial Services ISAC, an initiative which is an example of public-private partnership. It is a form of cooperation between law enforcement, the Hungarian banking association,

37 The New Internet, *Hungarian Defense Academy Looks to Fight Cyber Crime*, http://www.thenewnewinternet.com/2010/08/06/hungarian-defense-academy-looks-to-fight-cyber-crime/, 2010, [access: 17.03.2012].

38 The European Network and Information Security Agency, *Hungary…*, op. cit., p. 14.

39 Ibid, p. 15.

40 Air Webworld, *Harmonizing Legal Response To Cyber Crime: A Global Concern*, http://airwebworld.com/articles/index.php?article=1051, [access: 17.03.2012].

41 The European Network and Information Security Agency, *Hungary…*, op. cit., p.10.

the Hungarian Financial Regulatory Authority and individual banks. This public-private partnership allows for improvement of the participants' cyber security by conducting common exercises and exchanging recommendations and information on security in online banking.[42]

Conclusions

The period of the Hungarian Presidency showed that the country recognises and understands the importance of cyber security. By forming initiatives that are aimed at enhancing international cooperation in this field, not only within the EU but also at a transatlantic level, Hungary presented itself as a country which aspires to take the leading position in promoting cyber security within the EU. Awareness of the new cyber challenges is also visible in the security strategies, the most important security documents in the country.

Hungary is very active in the international environment when it comes to different institutions and organisations dedicated to cyber security issues (e.g. EGC Group, NATO and the EU projects). Some Hungarian initiatives, like those aimed at enhancing human factor (special classes at Zrinyi Defence Academy), show that the country understands the growing importance of cyber security. Additionally, the basic institution responsible for the cyber security, the NCC, is a well-organised one and with a great potential. There are plenty of other initiatives conducted by this organisation, which can serve as a good example, an inspiration for others (also for the V4 countries) and for cooperation between the states. It is also worth mentioning numerous interesting public-private initiatives aimed at improving cyber security (e.g. the Hungarian Financial Services, ISAC).

Practical situations, like the above-mentioned cyber exercises, exposed imperfections in Hungary's preparation for cyberdefence, showing that there is still a lot to be done. On the one hand, it must be pointed out that Hungary is not an exception and most of the entities are at the beginning of the road towards a solid cyber security system. On the other hand, exercised bare real problems that should not be neglected.

The government's achievements from the Hungarian Presidency period may be diminished because of its subsequent actions and decisions which were taken after that time. Controversial governmental changes and financial burdens which incriminated telecommunications services led to the conclusion that political decisions may prevail over the interest of cyber security. Especially the new rules that concern the governing of the National Agency for Data Protection may result in a loss of trust between the Internet users, which is a fundamental condition for the information society development.

Hungarian elites must keep in mind that it would be a big waste to squander both the potential of the Hungarian entities, which seem to recognise the needs and responsibilities of the modern world, as well as the potential developed by the government on its own.

42 Brunner, Suter, op. cit., p. 188.

7. Cyber Security in the European Union: Legal Aspects, Plans, Strategies, Actions

Tomasz Szatkowski

Introduction to the Role of the European Union in Fighting Cyberthreats

The European Union has adopted various policies regarding the issue of cyber security, sometimes in a not completely cohesive manner. Nonetheless, it is possible to generalise on its approach to the problem. To discuss the approach of the EU, a unique but already a classic political actor, the most significant feature stems from the issue of the actor attribution. It is implied by the fact that a response to a cyberattack is based on the existing institutional settings which differentiate, in terms of legal regime, threats posed by a criminal, terrorist or state actors.

This most popular approach to subcategorising cyberthreats is often criticised by many experts, since actor attribution poses a serious challenge in the ambiguous realm of the cyber space. It is suspected, moreover, that the most significant cyberpowers of state nature, employ non-state or even criminal actors to cover their involvement in unlawful activities against other countries. There have also been calls to employ the term of cyberterrorism very cautiously, as there are rarely direct victims of such an attack. Assimilating this dimension of cyberthreats with its "real life" equivalent would lead to application of a strict legal regime, with a possible encroachment on civil rights. Nonetheless, because of the fact that this division is most relevant to the distribution of EU competencies, it will have a certain role in this article.

Various experts have suggested however to use definitions based on sophistication and impact (e.g. US Air Force-Scientific Advisory Board intrusiveness-based division of Computer Network Operations into attack, exploitation and defence[1]) or on an approach to fighting the threat ("passive" dependent on enhancing resilience and stability[2] of the ICT structure or active "deterrence" based on cyber counter strike and, as such, requiring an actor attribution and being most relevant to the spectrum of cyberwar).[3]

1 Air Force Research Laboratory Information Directorate, *Cyber And Air Joint Effects Demonstration (CAAJED)*, March 2008, http://www.dtic.mil/cgibin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA481288, [access: 11.04.2012].

2 *European principles and guidelines for Internet resilience and stability*, v. of March 2011, http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf, , [access: 11.04.2012].

3 European Parliament, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Action within the EU*, a study, April 2011, p. 8.

The first two important features of the EU approach are its focus on cybercrime and cyberterrorism spectrum of the cyberthreats with a preference for undertakings enhancing the resilience of its critical ICT infrastructure as an implication to its goals of developing the information society. This approach is an implication of a division of the EU policy and its instruments according to its external or internal character, with the latter being equipped with stronger communitarian instruments. It might also be argued that it displays the EU's aversion to hard security issues. Nonetheless, experts argue that policies and methods devised for criminal and terrorist types of the cyberthreats, and for passive cyberdefence can likewise be essential in fighting the state-led attacks on information systems of the Member States.

External Aspects and Common Foreign and Security Policy and Common Security and Defence Policy Dimension

The institutional setting of the EU external actions has been strengthened by the Lisbon Treaty, which introduced the High Representative for Foreign Affairs and Security Policy, who acts as a "foreign minister of the EU" and conducts the Common Foreign and Security Policy (CFSP) being assisted by the European Union External Action Service and other bodies, such as the European Defence Agency (EDA).

The main weakness of this pillar of the EU policy, in comparison to its equivalents, is the fact that, as a principle, it is subject to an unanimity in decision making. This caveat applies not only to the prospect of establishing a common defence policy (Article 42.2 of the Treaty of the European Union – TEU), but also to any decision adopted by the Council in the area of CFSP.

This relative drawback is however addressed by special provisions which foresee a mechanism of Permanent Structure Cooperation (Article 42.6 TEU) for states "whose military capabilities fulfil higher criteria and which have made more binding commitments to one another with a view to the most demanding missions shall establish permanent structured cooperation within the Union framework." This mechanism can be established by a Council Decision (qualified majority vote) after consulting the High Representative. Protocol 10 to the Treaty specifies that this mechanism should be dedicated to mutual cooperation in areas of capabilities development, defence acquisition and in the activity of the EDA.[4]

The Union is equipped now with its own mutual assistance clause, which states that "if a Member State is the victim of armed aggression on its territory, the other Member States shall have towards it an obligation of aid and assistance by all the means in their power". (Article 42.7 TEU) However, the subsequent provisions of the Treaty limit the significance of this pledge as they state that these commitments should be consistent with Member States' obligations under the North Atlantic Treaty Organisation, which "for those states, which are members of it, remains the foundation of their collective defence and the forum for its implementation."

The actual scope of the EU's Common Security and Defence Policy (CSDP), which constitutes one of the instruments of the CFSP, is limited to the so called "Petersberg tasks" of crisis management nature: "joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation. All these tasks may contribute to the fight against terrorism, including by supporting third countries in combating terrorism in their territories" (Article 43.1 TEU).

Such setting and practice up to date suggest that NATO has an advantage over the EU in terms of hard security measures. This assumption is justified by the fact that it has not been possible to achieve an unanimous decision to establish a separate command structure for the CSDP.[5] In spite of the recurring ambitions of some political actors within the European Parliament or within the Council to achieve the "strategic autonomy" of the CSDP *vis-á-vis* NATO, it will rather remain defined by the principles of the Berlin Plus agreement. This arrangement is dedicated to cooperation in crisis management operations and establishes a principle of complementarity according to which the EU will lead only those operations which are not undertaken by NATO and for those purposes it will be able to use the Alliance's command structures. Therefore, it seems that the less sensitive and at the same time more binding Solidarity Clause (Article 222 Treaty on the Functioning of the European Union – TFEU) – another form of mutual commitment, envisaged for mutual assistance of Member States, under the coordination by the intergovernmental mechanisms of the Union, in case of an act of terrorism, man-made or natural disasters, may lend itself better for the EU common action in dimension of countering the cyberattacks.[6]

Summarising, such legal conditions imply that the overall EU's cyber security capabilities will have "passive" rather than "active" character.

So far, the issue of cyber security in the strategic documents of CFSP/CSDP has occurred in the report on the Implementation of the European Security Strategy submitted in pre-Lisbon setting by the Secretary General/High Representative to the European Council in December 2008. The EU military authorities also began to examine feasibility of developing a common doctrine on Computer Network Operations.[7] Given the above mentioned limitations, such a doctrine would be limited only to aspects pertaining to certain CSDP crisis management operations and would not encompass the strategic level. According to Alexander Klimburg and Heli Tirmaa-Klaar, as long as the institutional framework of CSDP command and control capabilities remains weak, "the progress in the area of cyberdefence will be very slow, and can at best achieve only a limited joint integrated capability".[8]

It should however be noticed that significant progress and real added value of the EU is attainable in the area of capability development, procurement and R&D. The recent EU's "pooling and sharing" initiative is geared in a pragmatic way for methods of achieving the economy of scale in defence capabilities development, acquisition and maintenance, which could later be utilised both for NATO and EU tasks and missions. The EDA has an ambition and is being positioned to achieve the role of a facilitator for such projects. The account of successes is limited so far, nonetheless, a couple of research

4 European Parliament, *Lisbon Treaty and its implications on CFSP/CSDP*, a policy briefing, 1 September 2009, p. 6.

5 C. M. O'Donnell, *Poland's U-Turn on European defence – a missed opportunity?*, CER Policy Brief, March 2012.

6 More on the solidarity clause in: S. Myrdal, M. Rhinard, *Empty Letter or Effective Tool? An Analysis of Article 222 of the Treaty on the Functioning of the European Union*, "Occasional Paper" 2/2010, Swedish Institute of International Affairs. www.ui.se.

7 European Parliament, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Action within the EU*, a study, April 2011, p. 34.

8 Ibid., p. 35.

programmes in the field of cyber security have been coordinated by the EDA. Likewise, there is some room for progress in the area of R&D for cyberdefence technologies. The Lisbon Treaty has opened a way to link defence research with general EU research policy and there are prospects that this area will be funded in the new EU's framework research funding program Horizon 2020 starting from 2014.[9] In the future, such projects could be led by the EDA, or be overseen by the Commission with its involvement. A provision of article 185 of the Treaty on the Functioning of the European Union also offers a basis for the Union to contribute to manage and implement programs "undertaken by several Member States". This offers an interesting option of support for more significant projects of regional cooperation in the area of cyber security technologies research.

The Area of Cybercrime and Cyberterrorism

The Treaty of Lisbon has transformed the scope of the application of the "third pillar" (police and judicial cooperation in criminal matters), which was governed by intergovernmental cooperation, into the dimension of shared responsibility of the EU and Member States (as an area of freedom, security and justice), where nonetheless, "Member States cannot exercise competence in areas where the Union has done so." This equips the Union with much better way in comparison to the dimension of the CFSP/CSDP. This area comes under the purview of the European Commissioner for Justice, Fundamental Rights and Citizenship and the European Commissioner for Home Affairs. They deal with matters of: EU citizenship; combating discrimination, drugs, organised crime, terrorism, human trafficking; free movement of people, asylum and immigration; judicial cooperation in civil and criminal matters; police and customs cooperation; and these matters in the acceding countries. The DG for Justice and DG Home Affairs constitute the European Commission's departments that administrate those areas.

Key legislation on cybercrime dates back to the 2005 when Council Framework Decision on Attacks against Information Systems was adopted.[10] It requires all Member States to introduce legislation to enhance cooperation between judicial and other competent authorities through approximating the rules on criminal law in the area of attacks against information systems dealing with most prominent kinds of cyberthreats and requiring penalisation of such actions like "illegal access to information systems", "illegal system interference" and "illegal data interference". The European Commission has initiated in 2010 a procedure of amending this directive so as to expand its scope as a result of "the emergence of large-scale simultaneous attacks against information systems and increased criminal use of the so-called "botnets".[11]

Another important pre-Lisbon piece of legislation is the European Data Retention Directive from 2007 which introduced a requirement of legislation obliging telecommunications and internet services providers to retain data on user traffic.

A communication of the European Commission from 2007 "Towards a general policy on the fight against cybercrime" aimed at drawing up of a general policy for improving the coordination of the fight against cybercrime at European and international levels. It sets out a package of measures to address this phenomenon and to improve cooperation between the various operators at the EU level, such as the improved law enforcement cooperation, better coordination between the Member States, political and legal cooperation with third countries, reinforced dialogue with industry, awareness-raising as well as training and research.

Another important pillar of the pre-Lisbon cyber security measures formed a part of the EU counterterrorism strategy and included fighting the radicalisation of content in the Internet (Counter-radicalisation strategy from 2005).[12]

A new thrust to the EU activities came with the adoption of the Lisbon Treaty. The Swedish Presidency, which preceded its entry into force, put issues of cyber security very high on its agenda (as a part of the "Stockholm programme")[13], calling for development of better and more resilient network information security measures, improving capabilities to deal with cyberattacks, adopting Council of Europe Cybercrime convention and accenting the importance of other activities between the EU institutions, Member State governments and private sector, such as information exchange. Another important political step initiated by the Swedish presidency was its idea to adopt the European Internal Security Strategy. This initiative came to fruition in October 2010. Within one of its five strategic objectives, called "Raise levels of security for citizens and businesses in cyber space" the strategy states that "rapidly evolving information technologies also create new forms of threats. To combat cybercrime, EU countries must collaborate at EU level to take further action:

- building capacity in law enforcement and the judiciary: an EU cybercrime centre for cooperation between EU countries and EU institutions will be established, and EU countries' capacities for investigation and prosecution will be developed;
- working with industry to empower and protect citizens: a system for reporting cybercrime incidents will be set up, and guidelines on cooperation for treating illegal internet content will be drawn up;
- improving capability for dealing with cyberattacks: a network of national and EU level Computer Emergency Response Teams (CERTs) and a European Information and Alert System (EISAS) will be set up".[14]

At the end of March 2012, the European Commission issued a proposal for establishment of the European Cybercrime Centre which will be operational by 1 January 2013 and will become its main operational institution to facilitate policy on cybercrime. It is expected to pool expertise and information, support criminal investigations and promote EU-wide solutions, while raising awareness of cybercrime issues across the Union. The Centre will serve as the European information hub on cybercrime, developing most advanced capabilities to support investigations in the EU and building capacity to combat cybercrime through training, awareness raising and delivering best practice on cybercrime investigations. The Centre is also expected to provide a networking role for experts to combat and prevent cybercrime and online child sexual abuse.

9 European Parliament, *The impact of the financial crisis on European Defence*, a study, April 2011, p. 56.

10 *Council Framework Decision on attacks against information systems*, 2005/222/JHA, 24 February 2005.

11 *Proposal for a Directive of the European Parliament and of the Council attacks against information systems and repealing Council Framework Decision 2005/222/JHA*.

12 European Commission, *Towards a general policy on the fight against cyber crime*, COM (2007) 267 final, 22 May 2007.

13 Council of the European Union *The Stockholm Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, 2 December 2009.

14 *Summary of the EU Internal Strategy*, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0050_en.htm, [access: 11.04.2012].

Security and Resilience of Network and Infrastructure

This area is defined within the EU as Network and Information Security (NIS) and is governed by different levels of shared competencies of the European Union, from a more robust one (from the EU institutions' point of view) where "Member States cannot exercise competence in areas where the Union has done so" (consumer protection, trans-European networks) to one where "Union exercise of competence shall not result in Member States being prevented from exercising theirs in:" (research, technological development). The DG INFSO (Directorate General for Information Society and Media) is currently responsible for coordinating this policy area within the European Commission. It should be noted, that the main task of this Directorate is the development of the cyber space as an enabling factor for society's and industry's development by:

- achieving the digital single market,
- reinforcing Europe's competitiveness by increasing investment in ICT research and innovation,
- promoting the access and use of ICT to the benefit of EU society.[15]

"Digital Agenda for Europe" (DAE)[16] constitutes its main policy document related to those issues, and some of its provisions are also encompassed by the more comprehensive Europe 2020 Strategy.[17]

The attacks on Estonia in 2007 prompted the DG INFSO to launch the EU's Critical Information Infrastructure Protection (CIIP) Policy. On 30 March 2009, the Commission adopted the Communication on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyberattacks and cyberdisruptions: enhancing preparedness, security and resilience" setting out a plan (the "CIIP action plan") to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructure.[18] The aim was to stimulate and support the development of a high level of preparedness, security and resilience capabilities both at the national and European level. This step has been met with support of the Council in 2009. The document envisaged a number of initiatives to achieve the desired goals, such as working groups, information exchange and a mechanism called the European Public Private Partnership for Resilience (EP3R), which constitutes a public-private partnership and forms another platform for transatlantic cooperation, and last but not least, the setting-up of the European Information Sharing and Alert and System (EISAS) and the organisation of pan-European exercises to manage major cyberincidents. It calls also upon the Member States to establish their Computer Emergency Response Teams by the end of 2012. In March 2011 DG INFSO presented also a useful, non-binding document: Principles and Guidelines for Internet Resilience and Stability.

The DAE also constitutes a follow up to the NIS dimension. Except for calling for the abovementioned revision of the Council Framework Decision on Attacks against Information Systems, it put an emphasis on the need for all stakeholders to join their forces in a holistic effort to ensure the trust and security within the Internet also by enhancing resilience of ICT infrastructures, focusing on prevention, preparedness and awareness, as well as to develop effective and coordinated mechanisms to respond to new and increasingly sophisticated forms of cyberattacks and cybercrime. In an afterthought to the DAE, the Commission tabled a proposal for a new mandate to strengthen and modernise the European Network and Information Security Agency (ENISA) in order to boost trust and network security. Strengthening and modernising the ENISA will help the EU, Member States and private stakeholders develop their capabilities and preparedness to prevent, detect and respond to cyber security challenges.

The ENISA, which acted until 2009 in mostly advisory, research related role, assists the Commission, the Member States, as well as private actors in meeting the requirements of network and information security, including the present and future EU legislation. The ENISA becomes a centre of expertise for both the Member States and the EU Institutions to seek advice on matters related to network and information security. Recent achievements (coordinating the Pan-European Exercises and facilitating the discussions with private sector and international partners, a task to set up CERT for EU institutions) gives this institution a major role as a an actor of European cyber security.

Recent Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber security", adopted on 31 March 2011, is particularly important as it takes stock of results achieved since 2009. It builds on existing policy initiatives, in particular the Digital Agenda for Europe, Stockholm Action Plan and Internal Security Strategy. In accordance with its title, it also indicates the next steps at the European and International level. The Communication observes an evolving nature of the threat underscoring three important more advanced forms which concentrate on the higher end of its spectrum:

- exploitation purposes (political espionage),
- disruption purposes (such as Distributed Denial of Service attacks or spamming generated via botnets, and Stuxnet),
- destruction purposes (fortunately not yet materialised but cannot be ruled out in the future).

The Communication calls for an international approach and cooperation, stating that "a purely European approach is not sufficient to address the challenges ahead. Although the objective of building a coherent and cooperative approach within the EU remains as important ever, it needs to be embedded into a global coordination strategy reaching out to key partners, be they individual nations or relevant international organisations." The next five pillars of the new CIIP Action Plan envisage:

1. Preparedness and prevention, which encompasses the ENISA's coordinative and fostering role *vis-à-vis* Member State CERTs, further efforts within the EP3R, and the European Forum for Member States.
2. Detection and response concentrates on the European Information Sharing and Alert System (EISAS) where the ENISA is tasked to support MS by developing basic services needed for the national ISAS and to develop "interoperability services".
3. Mitigation and recovery which encompasses both national contingency plans and exercises and the Pan-European exercise on large-scale network security incidents.
4. International Cooperation – promoting the European principles and guidelines for Internet resilience and stability on international forums as well as organising global cyberincident exercises.
5. Criteria for European Critical Infrastructures in the ICT sector.

15 *DG INFSO mission*, http://ec.europa.eu/dgs/information_society/see_more/index_en.htm#mission, [access: 11.04.2012].
16 European Commission, *A Digital Agenda for Europe*, COM (2010) 245 final/2, 26 August 2010.
17 European Commission, *Europe 2020, a strategy for smart, sustainable and inclusive growth* COM (2010) 2020 final, 3 March 2010.
18 *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, COM (2009) 149 final, 30 March 2009.

Other actions than the ones mentioned before, described under the title "Way forward", include an action to develop "trust in cloud".

Another area of notable documents which impact on the NIS include: EU directive on Critical Infrastructure Protection from 2008, the purpose of which was to identify and designate the European Critical Infrastructure, and find a common way of enhancing its protection. This piece of legislation belongs to the energy and transport area of competence. It gives however a solid and sound framework to be expanded into the ICT sector. The envisaged actions encompass 'operator security plans', security liaison officers and mandatory reporting, as well as the exchange of sensitive information among the law enforcement authorities. Within the ICT sector, the continuously revised Telecommunications Package from 2009 harmonises legislation, with a special emphasis on enhancing security. It introduces, for instance, the requirement for telecom providers to provide information of 'incidents' (including cyberattacks) to ENISA. It puts also upon the Member States a requirement to apply risk management measures to ensure a minimum level of services and envisages other measures to ensure that Members adopt technical measures based on international standards.

Last but not least, it should also be noted that the DG INFSO released a non-binding document "Principles and Guidelines for Internet Resilience and Stability", usefully setting out vocabulary, definitions and proposing interpretation of basic notions from the subject.[19]

DG INFSO, together with DG Home Affairs is also tasked to represent the Commission within the Working Group on Cyber Security and Cyber Crime. This Working Group, established at the EU-US Summit in November 2010 is devised to develop collaborative approaches to a wide range of cyber security and cybercrime issues, such as expanding incident response management capabilities, engaging the private sector and other actors, joint awareness-raising activities and fighting child pornography.

This Working Group serves as a very good model for reaching out to other countries or organisations which are concerned with similar cyberissues.[20]

Conclusions

The EU has achieved a considerable merit by providing new standard in the area of penalisation and cooperation against the cybercrime. It has also been active and achieved undeniable progress in the area of enhancing resilience of the Network and Information Security. Its policy and capabilities in cyberwar remain very limited with the exception of prospects for funding the research in that area. The institutions of the Permanent Structure Cooperation and of a "delegated task" form an interesting basis for cooperating groups of Member States to benefit from the EU support.

19 *European principles and guidelines for Internet resilience and stability*, v. of March 2011, http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf, [access: 11.04.2012].

20 Europa.eu, EU Press release *Cyber security: EU and US strengthen transatlantic cooperation in face of mounting global cyber-security and cyber-crime threats*, 14 April 2011, http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246, [access: 11.04.2012].

8. NATO Fighting Cyberthreats

Joanna Świątkowska

From Cold War to Cyberwar

Cyberthreats have challenged the nation-states and bodies responsible for their security, as well as organisations and international alliances. They are an example of unconventional, asymmetric threat which has set NATO a task to remodel its traditional concepts, solutions and methods of cooperation and defence.

NATO is an organization with origins reaching the time of rivalry between two opposite camps: The United States of America and The Soviet Union. The Alliance had clearly defined tasks until the collapse of the system of the socialist countries; of which the most important one was to ensure members' safety and prevent hostile military action of the Soviet Union and its satellites. However, after the end of the Cold War, the previous main objective has become obsolete. This does not mean, however, that the Alliance itself has become redundant.

Paradoxically, all military operations carried out by NATO took place after 1990. It was due to the fact that many new, different kinds of threats appeared – instead of the previous main one. To prove how the new reality influenced NATO's actions, let us recall that the 5th Article promising collective defence in case of one of NATO's members being threatened, was used for the first time in history (and the last time so far) because of an unconventional attack – namely after the 11 September 2001 attacks. These terrorist acts brought attention on new actors, types of challenges and threats which, from now on, had to be faced by the Alliance and which had to be included in the key strategies.[1] NATO, at the very beginning of its activity, was focused only on conventional threats. All this shows how the way of thinking about security has changed throughout half of century.

Cyberthreats are a special category of untraditional challenges. They are new and, in fact, all their consequences still cannot be predicted. They can be a lethal tool in hands of organised criminal groups, but they can also be used by state and non-state actors (e.g. cyberterrorists) as well. Furthermore, they result in a problem of determining attribution and evaluating the

1 Let us mention about creating in 2010 NATO's Emerging Security Challenges Division, the purpose of which is to deal with unconventional threats, such as: terrorism, energy security and cyber security.

opponent's potential. Most of the time, it is not possible to clearly determine whether a given tool is an instrument designed for defensive or offensive actions. All this puts the Alliance in a new situation which demands an update of the previously known ways of operating i.e. rethinking the concepts of deterrence.[2] Moreover, the Alliance has no single, clearly defined threat, like it had at the beginning of its existence – now an attack from various directions should be expected.

Origins of NATO's Involvement in Building Cyber Security

The genesis of the Alliance's interest in cyber space protection reaches the '90s of the twentieth century, when NATO became involved in the Balkan conflict. A group of pro-Serbian hackers attacked the website infrastructure of the organisation in retaliation. As a result of these experiences, during the 2002 Prague Summit, the Alliance's authorities have decided to create a cyber security program, called "NATO Cyber Defence Programme", and initiated actions of appropriate entities. In that time, NATO Computer Incident Response Capability (NCIRC) – a body responsible for protecting the ICT infrastructure of the Alliance – was created as well.[3]

However, it was the incidents in Estonia which appeared to be the turning point. Massed attacks on the country's ICT infrastructure in 2007 initiated a serious discussion on cyber security, reconsidering NATO's cyber security-related tasks, and resulted in numerous organisational decisions. Even some radical voices calling for activation of Art. 5 of the Washington Treaty appeared. Cyberattacks in Estonia were also crucial due to the fact that until that moment NATO was focused mainly on defending its own ICT infrastructure. During the attacks in 2007, NATO sent to Estonia its expert, who was supposed to provide appropriate assistance.[4] From that time, the trend to promote IT security of the Alliance and its member countries has been developing.

As a result of these events, the Cooperative Cyber Defence Centre of Excellence (CCD COE) – an organisation established in 2006, being the centre for research[5] on cyber security – has obtained NATO's accreditation and is currently one of the key players involved in protection of cyber space. The mission of the CCD COE is to "increase the abilities, broaden cooperation and information exchange between NATO, NATO member states and other partners in the field of cyberdefence by training, research, exchange of experiences and consulting".[6] The most important aspects of research on cyberdefence are: political and legal solutions, concepts and strategies, tactical environment, critical IT infrastructure protection, organising exercises.[7]

Another summit in Bucharest (2008) brought the announcement of the Alliance's cyberdefence policy ("NATO Policy on Cyber Defence"). In the same year, NATO Cyber Defence Management Authority (CDMA) was established. This body is responsible i.e. for initiating and coordinating "immediate and effective cyberdefence when needed".[8] The CDMA is also the central point of management of the technical and political actions and exchanging information necessary for ensuring cyber security. In addition, it coordinates actions of NATO's entities involved in the Alliance's cyberdefence, as well as provides assistance for the victims of cyberattacks.[9] At the another summit in Strasbourg and Kehl in 2009, cyberdefence was officially incorporated to NATO exercises.[10]

In 2010 in Lisbon NATO's New Strategic Concept was introduced. For the first time in history, cyber security was included in such strategic document, and treated as a crucial element of the Alliance's activities. The Concept recommends development of NATO's possibilities in the area of preventing, detecting and defending from cyberattacks and building ability of effective recovery after attacks. NATO intends to introduce a coordinated method of cyberdefence including planning and possible aspects of development. In order to achieve this, elements of cyberdefence will be implemented to all of the Alliance's tasks. At the same time, The North Atlantic Council has been obliged to develop an improved plan of NATO's cyberdefence.[11]

Though "self-defence" is a core task, the Alliance's engagement in coordinating member countries'actions for cyberdefence is becoming increasingly visible. The document is related to an implementation document called the Action Plan, which defines NATO's and Allies' detailed tasks and activities in the field of ensuring cyber security.[12]

Main Assumptions of Alliance's Cyberdefence

NATO's principal focus is on the protection of its own ICT systems and networks. The Alliance believes that integrity and continuous functioning of its ICT system must be guaranteed in order to perform its core tasks of collective defence and crisis management. Cyber security is therefore a mean to an end, but at the same time – it is a purpose itself. NATO bases its cyberdefence efforts on tasks concerning: prevention, resilience and non-duplication.[13]

Though "self-defence" is a core task, the Allliance's engagement in coordinating member countries' actions for cyberdefence is becoming increasingly visible. The fact that it is the national authorities and adequate state bodies who are responsible for cyber security in the first place, still remains the unquestionable and core rule. But it is also commonly known that NATO is protected from cyberattacks as efficient as its weakest member is. That is why NATO undertakes efforts to coordinate cyberdefence of its member states.

2 More: K. Geers, *The Challenge of Cyber Attack Deterrence*, "Computer Law & Security Review", 26(3) 2010.
3 S. Myrli, *173 DSCFC 09 E bis – NATO and Cyber Defence*, http://www.nato-pa.int/default.Asp?SHORTCUT=1782, [access: 07.04.2012].
4 Ibid.
5 From the legal point of view, the facility is an international military organisation.
6 EESTI.pl, *Zabiegi Estonii o lokalizowanie instytucji międzynarodowych na terenie kraju*, http://www.eesti.pl/index.php?dzial=panstwo&strona=instytucje_miedzynarodowe, [access: 05.04.2012].
7 Ibid.
8 Myrli, op. cit., p. 173.
9 Ibid.
10 Ibid.
11 NATO, *Defending the networks. The NATO Policy on Cyber Defence*, http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf, [access: 04.04.2012].
12 Ibid.
13 Ibid.

One of those tasks concentrates on implementing cyberdefence into the national activities related to security, including the solutions proposed by "NATO's Defence Planning Process". NATO also develops minimum requirements for those national networks that are connected to or process NATO information.[14] The first step is therefore identification of the critical network elements. NATO intends to provide assistance for the Allies in meeting the obligations if requested.[15]

At present, the most important provision, on the Alliance's response to cyberattack upon any of NATO members, included in the new Strategic Concept, says that in case of an attack, any collective defence response is subject to decisions of the North Atlantic Council. In addition, NATO shall provide coordinated assistance to any Ally being a victim of a cyberattack. Within the context of these assumptions, cyberaspects will be integrated into NATO Crisis Management procedures and the consultation mechanisms, early warning, situational awareness and information-sharing among the Allies will be enhanced. International cooperation with private and academic entities is also a very important aspect.[16]

Cyberattacks and the Three Musketeers Rule

The abovementioned provisions of "possible" application of Art. 5 in case of cyberattacks, as well as providing support for NATO member countries, are a starting point for a deeper analysis of the Alliance's policy on cyber security. Such described definition of obligations leaves NATO room for manoeuvre as well as the possibility of flexible response. This is important at least in the context of cyberattack characteristics, for example, in the context of difficulties in determining their potential impact and consequences. Was blocking Estonia's most important websites enough to disturb functioning of the state and should that event have initiated the collective defence rule? Most experts think it was not enough and they believe that such a radical response should be retained for possible attacks bringing heavier losses.

Moreover, the situation in Estonia has shown that it is very difficult to prove one's responsibility for cyberaggression, despite the fact that there is strong circumstantial evidence indicating the possible aggressors. Without solving the attribution problem it is impossible to use Art. 5. Therefore, not applying rigid rules that would determine which attack and when starts a collective response, seems a good solution. At the same time, signalising the possibility of conducting collective actions serves as a warning factor. The problem is, of course, much more complex because cyberattacks can be components of conventional attacks, which significantly changes the situation. Keeping in mind the complexity of the issue, it seems that the decision to consider each problem separately is right. The possible application of Art. 5 is additionally supplemented by the Alliance's declaration on providing support and coordinating actions in case of an incident. A clear indication of execution of Art. 4[17] is therefore a good additional protection.

14 Development of minimum requirements for countries which are not NATO's members but which cooperate with NATO is also planned.

15 NATO, *Defending the networks. The NATO Policy on Cyber Defence. . .*, op. cit.

16 Ibid.

17 *The North Atlantic Treaty*, Article 4: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened".

It should be emphasised that NATO's actions have another advantage which makes this organisation one of the most effective in ensuring cyber security. The Alliance is an agreement between countries which have a similar vision of the world and security. These like-minded partners provide mutual assistance by similar risk evaluation and action prioritisation. In the face of activities of the international community in the area of cyberconflicts, which are non-regulated by any treaty, it appears that the organisation could provide effective assistance to its members without the unnecessary relying on non-existing or non-precise procedures. It is especially important for those countries which have not developed their own legal framework and strategy in case of cyberattacks, which in case of problems reduces their chance for receiving support by the international community. Instant NATO assistance may therefore be crucial.[18]

Cyber Smart Defence

Smart Defence is NATO initiative developed in response to the reduction of financial funds for military issues. The economic crisis has caused the need to cut and rationalise expenses. It was an impulse to introduce innovative solutions which would take budget cuts into account and, at the same time, they would not lead to NATO's defence capabilities reduction. The Smart Defence initiative is based on encouraging member countries to closer and more coordinated cooperation in the field of development, as well as gaining and maintaining military capabilities, which would enable them to meet today's safety challenges. The essential principle is therefore to coordinate all actions on the basis of "pool and share" rule, which makes Allies share the best solutions with others. The countries can focus exclusively on their own, specialised areas and introduce them as their contribution and proposition for others and, simultaneously, profit from other's specialisations. Such activity enables to increase efficiency and reduce costs.[19] The cooperation is related to a wide range of projects such as common use of military units and weapons, training, planning, logistics, setting priorities.[20] This proposition is interesting especially for "smaller" players, as it enables building their own, individual portfolio in the chain of joint projects, and therefore makes their position stronger. The project is also a chance for building coalitions and initiating strategic cooperation, for example, between the countries which share the same challenges, which are joined by geographical proximity, complementary specialisations or even culture background.[21]

The Smart Defence initiative can be very attractive in the context of building capabilities associated with cyber space. It provides a chance for close cooperation which promotes share of information, experience and, what is very important, collective development of technological solutions.[22]

18 More : E. Tikk, *Global Cyber Security – Thinking About The Niche for NATO*, "SAIS Review", Volume 30, Number 2, Summer-Fall 2010.

19 NATO, *Smart Defence*, http://www.nato.int/cps/en/SID-8A152E11-04F93301/natolive/topics_84268.htm, [access: 07.04.2012].

20 Senat.gov, *Senator Bogdan Klich uczestniczy w seminarium NATO*, http://www.senat.gov.pl/wydarzenia/art,154.html, [access: 07.04.2012].

21 Involvement of the non-state agents like private companies, academic sector etc. is also required.

22 There is a similar project within the Alliance – The NATO Consultation, Command and Control Agency – NC3A – which is responsible for many technological projects within the NATO, i.e. creating cyber space defense system. Bodies which cooperate with the Agency can reduce costs, but above all, they can develop and introduce advanced technologies in areas like: command and control system (C2), anti-cyberattack systems, intelligence and reconnaissance information exchange system (ISR) and supporting coalition's interoperating

Building a joint Visegrad Group countries "front" within NATO, which would specialise in cyber security, is therefore worth considering. These countries are united by historical experiences (especially those form the last century), geopolitical proximity, similar potential, priorities and challenges. Projects which require mutual understanding and trust are easier to develop on such foundation.

Currently, there is ongoing work on developing the priority areas within the Smart Defence initiative. These priorities will be introduced during the Summit in Chicago in May 2012. This publication will be released after the event, but nevertheless it seems that the Visegrad Group countries should force the inclusion of the cyber security component within the Smart Defence and create their own, joint projects in this area in the future.

Conclusion

NATO is a political and military alliance which now has the chance to play the key-role in the field of cyber security, especially in regard to cyberterrorism and cyberwar. Its potential arises from the organisation's character and its great authority. The Alliance has already made important steps in developing ways of ensuring cyber space security. NATO's projects are a good supplementation for actions undertaken by other international organisations which are responsible for different cyber security areas. NATO introduces many security-building instruments for its members and it also provides space where it is easier to accomplish any collective initiatives. The Visegrad Group countries should perceive and take full advantage of these opportunities.

information exchange system – Source: Polska Zbrojna, *Podpisano umowę o współpracy z Agencją NATO ds. C3*, http://polska-zbrojna.pl/index.php?option=com_content&view=article&id=11483:podpisano-umow-o-wspopracy-z-agencj-nato-ds-c3-&catid=55:z-kraju&Itemid=104, [access: 07.04.2012].

Recommendations

Tomas Rezek, Tomasz Szatkowski, Joanna Świątkowska, Jozef Vyskoč, Maciej Ziarek

The Most Important Recommendations

- Common understanding of the fundamental cyber security framework needs to be ensured. The process includes, among others, consideration of key players, definition of basic notions and fundamental security goals as well as limitations which need to be respected (e.g. privacy preservation).

- It must be understood that operation security is just a part of the whole effort necessary to ensure a proper protection and that the quality of design, implementation and testing of a system also contribute to the overall level of security. Therefore, an adjustment of requirements and procedures for the ICT procurement ought to reflect that.

- It is essential to admit that establishing the basic jurisdiction and administration for the cyber security issues is not final, but just the first step, and that such basic framework needs to be complemented by properly qualified people. Apart from that, the building of permanent structures is not the only option as it is possible to make use of crowdsourcing, *ad-hoc* working groups, independent think-tanks, etc. Additionally, it is recommended to consider supporting cyber security-related competitions or awards for the contributions in the area of cyber security.

- It is recommended to finish the implementation. Despite the fact that the V4 countries have a very broad theoretical and political framework to improve cyber security, the implementation is either delayed or postponed practically in every country. This may lead to some potential problems as the image of a country is overly positive considering cyber security – cyberdefence strategies, action plans or dedicated offices do exist, but actually there are only minor changes in the situation as the action plans are delayed or not adhered to, the dedicated offices are understaffed or without authorities and the strategies are not implemented.

- It is postulated to provide a regular, independent and qualified assessment on the country's preparation for dealing with the cyber security issues; at least an Executive Summary of the assessment has to be published.

- There is a need to organise security exercises, aimed not only at simple technical threats (like denial-of-service attacks), but also at the threats which require the involvement of the decision-makers (e.g. a compromised private key of an accredited certification authority, discovered security flaw in an eID/ePassport or important eGovernment system taken down with a subsequent attempt to blackmail government). Issues with regard to dealing with public relations matters need to be included in such exercises.

- There is a need for cooperation during incidents – cyberattacks are completely different from other types of attacks. The attack itself may not be a one-time incident, but it may last for hours or even days. In such cases, an international cooperation is crucial to defend the critical infrastructure and to quickly restore the attacked services. The V4 countries can unite efforts by creating scenarios of a mutual cooperation in case of an attack. This cooperation may consist of Internet traffic transfer to other servers, resources for analysis, etc.

- It is crucial to admit that there are different categories of a cyber security expertise (e.g. skills in technical security do not automatically encompass an ability to analyze trends or to prepare qualified strategic documents) and to ensure initial and regular assessments of a pool of available cyber security experts. Especially in the cases of a small actual number of specific expertises there should be a possibility of an urgent international cooperation (a preliminary agreement to allow that should be ensured).

- Education must be improved – cyber security is a problem not only of the global companies and military structures. Cyber security is created by every individual who is active in the cyber space. Therefore, it is necessary to enhance the awareness of risks related to the cyber space and spread the knowledge of the best practices as well as basic security principles and their use in practice.

Other Proposals

- Initiatives like the 'Visegrád Workshop', tightening the international cooperation and communication in the field of critical information infrastructure protection between Poland, Slovakia, Hungary and the Czech Republic should become a regular event. Furthermore, apart from national entities responsible for the CIIP, also its owners and operators should be invited to participate.

- There is a strong need for the public-private cooperation within each of the V4 countries as well as on the cross-national sectoral working groups level. Additionally, private entities should be strongly involved in the process of the cyber space protection.

- The V4 countries should exploit the opportunities offered by the Smart Defense initiative and start working within it towards a common building capacity to ensure the protection of the cyber space.

- Countries which have not ratified the Council of Europe Convention on Cybercrime yet (Poland, the Czech Republic) are recommended to do that.

- The V4 countries should support the involvement of private sector in the Cyber Europe exercises and exercises organised by NATO.

- The V4 countries should jointly explore the utility for the benefits of the regional cooperation on cyber security, of the mechanism offered by the European Treaties such as permanent structured cooperation, or a EU's provision to a task undertaken by several Member States.

- The V4 countries should support the inclusion of the provisions related to the cyberthreats to the new edition of the European Security Strategy.

- There is a need for establishing a new comprehensive EU cyber security strategy that would encompass all the dimensions of the EU action in this field.

- The V4 Group should support establishing a body (e.g. EU Cyber Security Coordinator) for the purpose of coordinating various aspects of the EU cyber security policy. Optionally, the responsibilities of the above-mentioned entity can be attributed to an already existing structure.

- Developing the CSDP doctrine on cyberwar, that would encompass the issue of information operations and would be compatible to relevant NATO procedures is recommended.

- The V4 Group should postulate the inclusion of funding the tasks related to cyber security into various EU's funding mechanisms (e.g. cohesion policy).

- There is a need for funding a cyber security related research within the Horizon 2020 programme.

Authors

Tomas Rezek

PhD candidate in the Department of International Relations in the Faculty of Social Science at the Charles University in Prague. He graduated in International Trade and Commercial Communication at the University of Economics in Prague in 2009. Since 2009 he has been working for global consulting company in the field of ICT and financial institutions. Since 2012 he is with the Association for International Affairs, Prague based think tank, where he is responsible for cyber security agenda.

Tomasz Szatkowski

lawyer and a graduate of the Department of War Studies at the King's College, London. He used to hold the positions of vice president of the Bumar Group, board member and acting president of TVP S.A. He has been also working on various position related to defence, industrial, and intelligence policy at the Chancellery of the Prime Minister of the Republic of Poland, and as a policy adviser on security and defence for the ECR Group at the European Parliament, an expert of the Kosciuszko Institute. He wrote a number of articles related to prospects of regional security and defence cooperation, including partaking in the Visehrad Security Cooperation Initiative in 2010.

Joanna Świątkowska

political scientist, an expert of the Kosciuszko Institute. Graduate of the Pedagogical University of Cracow and Dalarna University in Sweden. Currently, a PhD candidate of Political Science at the Pedagogical University of Cracow. Specialist in the field of security and defense. In the Kosciuszko Institute she is responsible for cyber security agenda.

Jozef Vyskoč

has studied theoretical cybernetics at the Faculty of Natural Sciences of Commenius University, Bratislava, and computer science at the University of Rochester, NY, USA. PhD. in management received from the Faculty of Management of Commenius University, Bratislava. Information security specialist and auditor of VaF, s.r.o. consulting company. Leads information security courses at the Faculty of Management of Commenius University, Bratislava, and Faculty of Informatics of Paneuropean University, Bratislava. First

(in 1996) Certified Information Systems Auditor (CISA) in Slovakia. From 2008 "Admitted technical expert" for the European Privacy Seal (the only one in Slovakia).

Maciej Ziarek

is a graduate of Archival Sciences and Documentation Management at Nicolaus Copernicus University in Toruń, as well as of Computer Science at the Academy of Information Technology in Bydgoszcz. In 2009, Maciej begun his work in Kaspersky Lab Poland as a 'threat analyst'. Maciej's personal interests are cryptology and security of mobile operating systems.

PUBLISHER

The Kosciuszko Institute – a think-tank creating new ideas for Poland and Europe – is an independent and non-governmental research institute founded in 2000 as a non-profit organization. The mission of the Kosciuszko Institute is to contribute to the social and economic development of Poland – an active member of the European Union and a partner of the Euro-Atlantic Alliance. The Kosciuszko Institute strives to be a leader of positive changes, to create and to promote the best solutions not only for Poland but also for Europe as well as for neighbouring countries which are now in the process of building states based on the rule of law, civil society and a free market economy. www.ik.org.pl

PARTNERS

The Association for International Affairs is a non-governmental organization founded to promote research and education in the field of international relations. Thanks to its activities and more than ten-year tradition, Association has established itself as the preeminent independent foreign policy think-tank in the Czech Republic. The Association facilitates expression and realization of ideas, thoughts and projects in order to increase education, mutual understanding and tolerance among the people. The Association represents a unique forum in which academics, business people, policy makers, diplomats, the media and NGOs can interact in an impartial environment. www.amo.cz

Századvég Economic Research Ltd. aims to perform and conduct high-standard, scientifically elaborated economic and social research. To promote such new, economy-related axioms to become embedded can be done only by an institution of strong professional foundations and weighty scientific background, that is always capable of acting both with due measure and authority. The research institute shoulders the responsibility for the preparation of economic analyses on the level of companies, various sectors, and the national economy. Furthermore, the institute must tackle the implementation of such evaluations of economic policy that are suitable for assessing and analysing the foreseeable impact of economic regulations and planned governmental measures. www.szazadveg-eco.hu

The Slovak Atlantic Commission is an independent, non-partisan, non-governmental organization which deals with national and international security issues. Aim of the Slovak Atlantic Commission is to support constructive and active involvement of the Slovak Republic in international affairs with emphasis on cooperation in the Euro-Atlantic community, support of transatlantic cooperation and effective implementation of foreign and security policy of through building a net of individuals and institutions (state, non-governmental and private), unified in strong security community. The Slovak Atlantic Commission represents a net of leaders who bring ideas to power and give power to ideas. www.ata-sac.org

Kaspersky Lab. Kaspersky Lab is the largest antivirus company in Europe, providing protection against IT threats, along with viruses, spyware and crimeware, hackers, phishing and spam. The company is among the world's top four providers of protection for end-users. Kaspersky Lab products are characterised by an excellent detection ratio and very fast response time for appearance of new threats to home users, small and medium-size companies, corporations, as well as mobile device users. Kaspersky Lab technologies are used by many IT security providers throughout the world. The Polish branch office exists since 2001 and in September 2011 it celebrated its 10th anniversary. The latest information on the Internet threats is available in the Virus Encyclopedia prepared by Kaspersky Lab: www.viruslist.pl. www.kaspersky.pl

The *V4 Cooperation in Ensuring Cyber Security – Analysis and Recommendations* publication is a result of a project initiated by the Kosciuszko Institute. It is aimed at conducting scrutiny of the state of cyber security in the Czech Republic, Slovakia, Hungary and Poland, and at presenting recommendations that serve its reinforcement. Moreover, the publication includes the most important information on cyber space protection and a review of the actions in that area which are undertaken within NATO and the EU. It also constitutes a valuable material for the decision-makers who, on the basis of the presented analysis, have the opportunity to build proper political solutions. The publication serves as a source of knowledge for all of those interested in new trends in the international security sphere.

Publication is a part of the Kosciuszko Institute project *target: cyber security.*

target: cyber security

Partners

Asociace pro mezinárodní otázky
Association for International Affairs

SAC
SLOVAK ATLANTIC COMMISSION

KASPERSKY lab

SZÁZADVÉG
gazdaságkutató zrt.

Media patronage

EurActiv.pl

The publication is co-financed by the International Visegrad Fund

Visegrad Fund

ISBN: 978-83-93-10-93-6-4

THE KOSCIUSZKO INSTITUTE