PULASKI POLICY PAPERS
KOMENTARZ MIĘDZYNARODOWY PUŁASKIEGO
www.pulaski.pl ISSN 2080-8852 2/2011

Cybersecurity – a challenge to Poland

The Information and Communication Revolution has caused substantial consequences for all spheres of life. These include enabling the creation of brand new forms of business and changing the conditions in which traditional industries operate. It has also influenced the ways interpersonal relations are established and maintained, and the ways people spend their free time. Along with the huge impact on mass culture, it has had an effect on the development and transformation of the security environment of countries by generating new types of threats, mostly connected with the dependence of societies on various information and communication systems. These threats, still hardly recognised or analysed, are undergoing a constant evolution.

In the current issue of our policy papers Marcin Terlikowski analyses the challenges related to cybersecurity in Poland. "Due to the Polish international engagement, not only might military information and communication systems be a target for various attacks, a twilight zone of cyber crime has been developing as well. In recent years, a lot has been done to secure Polish cyberspace – thanks to the efforts of among others ABW (The Internal Security Agency) and computer science circles. Nonetheless, quite a few activities are still necessary."

I highly encourage you to read the new issue of the "Pulaski Policy Papers"!

Dominik Jankowski
Chief Editor of the "Pulaski Policy Papers"

Author

Marcin Terlikowski

Translated by:

Justyna Pado

Marcin Terlikowski

Marcin Terlikowski
Analyst at the Polish Institute of International Affairs, area of research: Common Security and Defence Policy, European defence industry and defence equipment market, cybersecurity and cyberwarfare.
Author of various papers and articles, covering inter alia ESDP missions and capabilities' development processes as well as the current problems of the European defence sector. Co-editor of a book on the role of cybersecurity in the modern state („Bezpieczeństwo teleinformatyczne państwa", Warsaw 2009).
Since 2007 PhD student at the Warsaw School of Economics, the dissertation subject: economic policies of EU members towards the defence sector.

The Information and Communication Revolution has caused substantial consequences for all spheres of life. These include enabling the creation of brand new forms of business and changing the conditions in which traditional industries operate. It has also influenced the ways interpersonal relations are established and maintained, and the ways people spend their free time. Along with the huge impact on mass culture, it has had an effect on the development and transformation of the security environment of countries by generating new types of threats, mostly connected with the dependence of societies on various information and communication systems. These threats, still hardly recognised or analysed, are undergoing a constant evolution.

Security in/of cyberspace

Information and communication security (in short: cybersecurity) is often defined in terms of maintaining access to information, its integrity (i.e., the certainty that it has not been changed without the knowledge and consent of a user) and confidentiality (i.e., the certainty that it will not be taken over by an unauthorized user). In brief, the correct functioning of information and communication systems (hereinafter ICT systems) is a basic condition of cybersecurity, which is assured only if those systems operate under the full control of the user and without any undesirable external interference. In this approach any actions – any random event or negligence – are regarded as ones which hamper the operating of ICT systems. However, it needs to be pointed out that cybersecurity does not only involve the security of the systems themselves (the security of 'cyberspace'), which also involves its protection against physical damage, but also the security of its users (security in 'cyberspace'). This second dimension regards technical issues as only one of a series of problems – a system working correctly may still generate threats for its users due to the content which is being processed and shared.
The list of threats to information and communication security includes mostly intentional acts, mainly creating and disseminating malicious software. Operating automatically, this kind of software (commonly, but often incorrectly described as 'computer viruses') modifies the functioning of systems infected by it without the knowledge and consent of its users. Remote, unauthorized manipulation of systems (commonly referred to as 'electronic attacks', e.g. attacks paralyzing the work of chosen systems or attacks aiming at stealing data, including internet fraud) is another example of such threats. From such a narrow perspective, information and communication security refers solely to the technical parameters of systems' operation, and does not include the wider context of their functioning – economic, social, political, etc. In times of rapidly expanding cyberspace such an approach is incomplete as the meaning of correct functioning of a single computer in a household or a small company's network is radically different from sustaining flawless operation of more complex systems e.g. steering the delivery of electricity or gas. Therefore, generalizing threats and particularly transferring experiences from small systems to large scale networks is partially wrong, and may lead to a false threat assessments.
The essence of the cybersecurity of the state are the potential results of failures in functioning of systems hit. Those results are in turn directly connected with a degree of dependence of socio-economic life on ICT systems. Therefore, from a perspective of a state, cybersecurity is virtually limited only to those systems whose dysfunction may cause widespread negative results for whole society. Special attention should be paid particularly to the networks which steer critical infrastructure, i.e. the networks used in transmission of utilities, industries, the financial sector, the military, and the telecommunication network of state administration and

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warsaw, Poland, tel. +48 22 658 04 01, office@pulaski.pl

intelligence services.
The destabilization of all these systems, in a radical scenario, could lead to serious consequences: a paralysis in normal functioning of the state (halt of energy and gas deliveries, disruption of communication within emergency and security services, disturbances in electronic systems used by banking and financial sector etc.), and even cause material damages (technical disasters in industry and transport, including potential contamination). Due to the substantial increase in the number of services provided on the Internet, also a paralysis of this network could bring very real consequences for the socio-economic life in the state. However, they would not be as serious as in the case of systems connected with critical infrastructure, and limit to a halt of popular services.
On the other hand, systems of individual users, even those belonging to larger companies, should not be a subject of states' close attention. An increase in the number of networks being under special protection would weaken the ability of state to act effectively against the most serious threats. This certainly does not mean, however, that no policies aiming to increase the degree of security of such systems (e.g. through updating law or conducting awareness campaigns), should not be implemented.

A hacker – a terrorist or a thief?

From a perspective of a state, another factor that determines the level of risk to information and communication security is its source: the perpetrator, and his/her motives. The first identified actors, who performed remote unauthorized manipulation to computer networks were 'hackers' – persons for whom overcoming security barriers of certain systems was a form of intellectual entertainment, undertaken individually. The level of threat posed by hackers is relatively low – their motives mostly consist in breaking into a system itself, without needing to destroy it (although there are also people who damage systems e.g. delete some of its data). Moreover, this kind of activity is not widespread now.
Political motives can also be behind threats to cybersecurity. In the nineties, for the first time a series of attacks which constituted a form of electronic protest was noted, e.g. in 1999 during NATO's air raids in Serbia, the Internet sites of the Alliance were hit and pro-Serbian and anti-American content was put on them (this type of political activity of hackers is known in the U.S. as 'hactivism'). Threats generated by hactivism are more serious than those of hackers but still they are limited to destroying WWW sites or paralysing e-mail servers. Thus, they do not pose a danger to a states as a whole, but merely to individual institutions and less important systems.
The birth of politically motivated electronic attacks has become a breaking point in thinking about cybersecurity of a state. The status of cyberspace as a new arena for a potential political conflict, engaging countries and non-state actors both using ICT systems in a function of weapon, has become commonly recognized (earlier on, an information warfare doctrine existed only in the military; it referred mostly to armed forces and a time of war).
Among the politically motivated threats, cyber-terrorism, generally defined as conducting terrorist attacks with the use of ICT systems, stands out as one of key challenges. As it was argued by many, in favourable conditions organized terrorist groups, having adequate financial and human resources at their disposal, could attack systems operating critical infrastructure. By manipulating these systems' functioning, such groups would be able at least to paralyze everyday life in the state (e.g. through cutting energy or water supplies), and even bring about serious material damage (e.g. causing technical and ecological catastrophes) or human losses (e.g. by causing accidents in electronically supervised transport systems). Nevertheless, no case of cyber terrorism has been observed so far. It seems that both the degree of complexity of such attacks and the uncertainty of their final effects discourage potential perpetrators – terrorist groups, which are mostly oriented towards obtaining quick results of their actions.

Quite different source of threats to cybersecurity of state are other governments. Having an easy access to financial resources, equipment and personnel necessary to conduct an electronic attack they may be even a more serious challenge for cybersecurity of other states than potential cyberterrorist groups. Nonetheless, currently the cyberespionage is the crucial threat posed by activity of state agents in cyberspace. The rising use of electronic channels for transmitting and processing classified information prompt the intelligence services from all over the world to conduct regular intelligence operations in cyberspace. This is particularly true of those countries which find themselves in a permanent conflict against the international community – they may resort to such spying activities on a large scale. In turn, the governments tangled in unsolved regional conflicts may even employ electronic sabotage, i.e. clandestinely destabilize or destroy certain systems of their political enemies.
A different type of motive is the economic motivation that drives the perpetrators of electronic attacks. The dynamic development of online financial and commercial services has enabled a boom in cybercrime. By means of various frauds and thefts of confidential data, cyber-criminals steal from their victims or extort money from them (another popular form of cyber crime is sending unwanted advertising mail, the so-called 'spam'). The relatively large profitability of cyber-crime is based on low costs and the great scale of the activity – if among several million fraud attempts, often conducted by means of only several computers, at least a per-mill result in success, criminals are able to rob thousands of individuals, and earn hundreds of thousands of dollars. From the perspective of an individual user, cybercrime is probably the most serious threat. However, cybercriminals do not have either the potential or the interest to act against a state and its institutions. While the threat to a state's national security should be regarded as small, this type of crime definitely needs to be fought.

Information and communication security 2011 A.D.

The period of the last three years has brought a series of events which require a re-definition of how the problem of cybersecurity of a state is perceived. First of them were the electronic attacks against Estonia in 2007, so far the biggest case of the so-called 'DDoS attack', consisting of the purposeful flooding of electronic devices by a stream of accidental data causing an overload and blockage. The attacks caused a paralysis of the Internet in Estonia, which hampered the functioning of hundreds of thousands of users in the entire country. Still, it did not bring about any major material or financial loss. The consequences of these events were however significant: the attacks became a red flag for many governments, exposed the weakness (or even the lack) of reaction mechanisms in these kinds of situations (a lack, weakness or wrong legal empowerment of the governmental Computer Security Incident Response Teams – CERTs). Soon after the attacks, NATO, the EU and among others, the U.S., the Great Britain, France and Germany set up institutions and procedures which were to enable a swift response from governments (and international organizations), should such a scenario be repeated again (e.g. NATO, during the Bucharest summit in 2008, accepted a special strategy on cybersecurity).
Attacks against Estonia also revealed another growing problem of cyberspace security – the huge scale of criminal activity. These attacks were possible thanks to special computer networks, amounting to hundreds of thousands of machines, and used daily to commit crimes (the so-called 'botnet' networks created mostly by means of computers belonging to various users, infected by certain malicious programs). Existence and growth of botnets is a evidence of a rapid increase in online criminal activity in the past few years. Today, one may rightfully speak about a global 'black market' where electronic tools used to commit electronic attacks are traded (e.g. one may buy botnets, viruses or revealed gaps in programs' protection mechanisms, the so-called 'exploits'). Complex services are also often offered e.g. data thefts on request. This market mostly serves the organized groups of cybercriminals which have made a healthy income out of online financial frauds and sending spam. What is however most

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warsaw, Poland, tel. +48 22 658 04 01, office@pulaski.pl

important – all those tools and services might be very well used by politically motivated actors, both non-state and governmental agencies.

The acts of mass electronic spying against the U.S., Germany, France and Norway (revealed gradually from 2008), have been another significant case of cybersecurity incident. Unidentified perpetrators (there were speculations about the source of these attacks being Chinese), undetected for a long period of time, gained access to various governmental networks from which they managed to copy data amounting to millions of pages of documents. Although there were no classified data among them (as the aggrieved governments were quick to underline), this was one of the greatest leaks of information in history. The attacks demonstrated the main feature that is characteristic to the electronic processing of information, i.e. the fact that a singular access to a system allows the theft of a substantial amount of data. Spying, associated some time ago with microprint and cryptogram, has gained now a mass character.

The after-effects for the perception of cyber security issue of the two events from the last weeks of 2010 (the Stuxnet and Wikileaks affairs) are still not fully clear. Experts have acknowledged the appearance of the 'Stuxnet' virus as the first time in history that a program has been created in order to damage a precisely defined electronic system – the program, above all, aimed at the systems steering specific industrial machines. Most important though, in the opinions of experts, 'Stuxnet' was created by a team of skilled programmers who had access to various electronic tools and confidential information (e.g. the architecture of the systems that was to be attacked). The motivation of its creators is unknown – the media has suggested that 'Stuxnet's' task was to paralyse the nuclear program of Iran. However, there is not sufficient evidence to prove it. Some opined that it was a peculiar demonstrator of technology or a test of a class of instruments, which would soon serve to conduct electronic wars. Regardless of the speculation, 'Stuxnet's' case shows that adequate financial and human resources already allow the creation of programs that are both selective and destructive, in practice serving as a sort of electronic weapon. There are no reasons to reject the assumption that these kinds of attacks may happen in the future.

In the case of the Wikileaks affair, the key security challenge is the potential for manipulation of public opinion thanks to having such a great amount of confidential information at one's disposal. Although the Department of State's cables that have been revealed so far do not include any sensational content, one cannot forget that in another potential leak information might be disclosed selectively or fictitious information might appear next to the real one. Such activities would allow the manipulation of public opinion, and in an extreme case, the manipulation of governments. Therefore, Wikileaks depicts well an interesting aspect of security 'in cyberspace': the correct operation of systems does not mean that the information is neither selectively chosen nor false and aims to stimulate certain opinions and behaviours. This dimension of cybersecurity is yet to receive serious in-depth analysis.

All the aspects of information and communication security described above refer to an equal degree to Poland, and should be considered when the main security policy assumptions and strategic goals are formulated. Due to its international engagement, not only might military information and communication systems be a target for various attacks, a twilight zone of cyber crime has been developing as well. In recent years, a lot has been done to secure Polish cyberspace – thanks to the efforts of among others ABW (The Internal Security Agency) and computer science circles. Nonetheless, quite a few activities are still necessary: Popularizing and systemizing the knowledge on information and communication security, conducting a coherent analyses of the significance of various aspects of this problem for national security, compiling a coherent model of tasks to improve the security of all systems key for the functioning of the state, increasing cooperation with the private sector, and also creating and practising crisis management mechanisms, which would clearly set the competences of institutions and state authorities with regard to most serious cybersecurity incidents.

The Casimir Pulaski Foundation

is an independent think tank which specializes in foreign policy, with a mission to promote freedom, equality and democracy, as well as to support actions of strengthening civil society. The foundation carries out activities both in Poland and abroad, among others in Central and Eastern Europe and in North America.

The Casimir Pulaski Foundation was founded due to political changes that took place in Poland after 1989. The principal values of Casimir Pulaski (freedom, justice and democracy) are an inspiration for every initiative undertaken by the Foundation. A few of the Foundations activities include: conducting scientific research, preparing publications and analyses, organizing seminaries and conferences, providing education and support for leaders www.instytutprzywodztwa.pl

The Foundation is the main organizer of the Warsaw Regional NGOs Congress www.warsawcongress.pl, the Academy of Young Diplomats www.akademia.diplomacy.pl and publisher of the Communication Platform for Non-Governmental Organizations www.non-gov.org

The Foundation also awards the Casimir Pulaski Prize "The Knight of Freedom" to outstanding people who have made a significant contribution in promoting democracy. So far the prizewinners were: Professor **Władysław Bartoszewski**, former Minister of Foreign Affairs of Poland, historian Professor **Norman Davies**, **Alaksandar Milinkiewicz**, leader of democratic opposition in Belarus, **Lech Wałęsa** and **Aleksander Kwaśniewski**, former Presidents of Poland as well as **Javier Solana**, former High Representative for Common Foreign and Security Policy, and **Valdas Adamkus**, former President of Lithuania.

The Casimir Pulaski Foundation is one of only two Polish institutions that have a partnership status with the Council of Europe. More about Foundation at: www.pulaski.pl

Pulaski Policy Papers

are analyses of foreign policy, international economy and domestic politics issues, essential for Poland. The papers are published both in Polish and English. Researchers willing to publish new articles in Pulaski Policy Papers are asked to contact the Chief Editor Mr **Dominik Jankowski** djankowski@pulaski.pl If you would like to receive new issues of PPP please add your e-mail at www.pulaski.pl

Fundacja im. Kazimierza Pulaskiego | Casimir Pulaski Foundation
ul. Oleandrów 6, 00-629 Warsaw, Poland, tel. +48 22 658 04 01, office@pulaski.pl