COL. PhD Eng. Maciej MARCZYK
LTC. PhD Eng. Bartosz BIERNACIK

m.marczyk@aon.edu.pl, ph (0048) 261- 813 - 357
b.biernacik@aon.edu.pl ph (0048) 261- 813 - 009

Address:
Nationals Defence University
Brig. Gen. Chruściela 103
00-910 Warsaw, Poland

RECONNAISSANCE OF CYBERSPACE IN TERMS OF MILITARY SECURITY OF THE STATE

Introduction

The beginning of the XXI century is characterized by fast development of information technology. The terms: "global village", " virtual world", cyberspace, information and communications technology era or information society occur in almost all spheres of human activity. Modern technologies commonly known as "high tech" permeate extensively every part of our life. Over the last years we have experienced a permanent invasion of services for an individual client as well as world corporations, from simple utility
software, entertainment software to electronic data exchange in any form of e-commerce, e-work, e-education, etc.

Protection of cyberspace constitutes one of the most often discussed topics concerning state security. The states, international organizations and other non-governmental entities realized that stability and global development of information society depend on open, reliable and first of all – safe cyberspace. Building up awareness of this phenomenon is on a par with rapid growth in computer incidents and new threats. Poland is also a target of cyberterrorist attacks. Similarly to other states, Poland faces the challenge of introducing legal and organizational changes to ensure required level of both military and non-military security in cyberspace and of citizens who operate in it[1].

Reconnaissance of cyberspace – military and legal aspects

Reconnaissance is a set of technical and socio - technical methods to obtain any possible information about the infrastructure and its personnel under attack. The tools most often used are: port and services scanners, Open Source Intelligence (helps us to find, select and acquire information from available public sources with use of , e.g.: Google Hacking), retrieving data from DNS systems.

Term "cyberspace" was used for the first time in 1984 by William Gibson in the novel *Burning Chrome*[2]. This is, generally, an imaginary space, created in people's minds. It is a very special space which is not limited with any time or geographical boundaries,

[1] Compare: *Doktryna cyberbezpieczeństwa RP*, BBN, Warsaw 22nd Jan.2015. , *Polityka ochrony cyberprzestrzeni RP*, MAC, Warsaw 25th Jun. 2013.
[2] The story *Burning Chrome* published in the American journal *Omni* in 1982. The term cyberspace was popularized by debut, the novel by William Gibson *Neuromance* published in 1984.

where no physic laws apply. It is the space impossible to localize and where time is counted differently. Moreover, it is populated by unreal creatures equivalent to their real ones, yet not the same.

In a cyberspace it is possible to change gender, age, race, education, character. In a humanistic discourse cyberspace is equivalent to the Internet, where computers or other digital media (e.g.: mobile telephony) connected to the network communicate. Generally, they are connected by the Internet. Cyberspace is also defined as a new type of social space where Internet users meet.

Another definition describes cyberspace as a virtual space created by collected resources on the Internet or as an illusion created by a special software and tools such as: glasses, helmets or gloves. In Polish language a term virtual has many meanings. In everyday usage virtual is opposite to real. The software used for reconnaissance are: Metasloit, Nessus, Nmap,, CoreInpact, GFI LandGuard, LophCrack, WebInspect.

Cyberspace and virtual reality

Cyberspace (Greek: Kybernetes - steersman or governor, control or regulate) recently prefix –cyber is associated with new, electronic technologies and means: informatics, interactive (defines everything that concerns computers). Cyberspace is a communication space created by Internet connections system. Cyberspace like telecommunication help network users communicate also in a real time. It is an open communication space created by computer and IT connections operating all over the world. This definition includes all electronic communication systems (also traditional telephony networks), which send information from numeric sources or information be numeric. Cyberspace is becoming a basic information
exchange channel.

Source: http://www.wsb.edu.pl/obszar-tematyczny,m,mwe,1519.html

Development of information society resulting from expansion of the Internet goes along with permeating another aspects of human activities in the cyberspace. All-over-the world range and immediate access from any place on the globe together with low costs of using encourage more and more entities (governments, institutions, companies) as well as individuals to move various elements of their everyday activity to a cyberspace. A lot of

Internet users cannot imagine life without fast access to current information and email, e-banking, e-shopping, online ticket booking or contact with a family and friends on social portals and the internet communicators. Available by a computer, mobile phones, tablets, even cars or refrigerators the internet has become one of the basic media along with electricity, gas and water. It has become a synonym of freedom of speech and free information flow and in some cases it is a tool of revolution and social changes.

Unfortunately, in the time when cyberspace is becoming a virtual reflection of physical reality, it is also permeated with the negative aspects of human activity. The Internet network created for purposes of scientific cooperation gives the sense of anonymity and is used by criminals, terrorists and some countries for illegal activities or aggression towards other entities.

Cybercriminals cause huge losses to companies, institutions and individuals all over the world. The analysis of 2011 estimated the losses of 388 mld USD and 69 % of adult Internet users were victims of cybercrime at least once in their lifetime. Generally, Internet users experienced attacks by harmful viruses and other software, Internet forgery, spoofing (phishing)[3].

Challenges and threats in cyberspace

Lack of universal definition for terms connected with cyber security generates problems to form legal regulations on national and international levels. Thus, protection of a global network is really difficult. There is no consensus also about universal definition of cyberweapon. Referring to the conventional weapon as a tool used or designed to cause damage (to systems, structures or living creatures) it can be agreed that cyberweapon is a computer code used or designed to cause similar damages.

[3] Spoofing (phishing) kind of scam where an intruder attempts to gain unauthorized access to a user's system or information by pretending to be the user. The main purpose is to trick the user into releasing sensitive information in order to gain access to one's bank account, computer system or to steal personal information, such as passwords. http://www.investopedia.com/terms/s/spoofing.asp (03.02.2015). Smishing is a type of phishing - an identity theft scheme which involves sending users text messages with a link to a fraudulent website or a phone number in an attempt to collect personal information.

Source: http://www.ppe./news-32387-cyberwojna_trwa_w_najlepsze_regin_infekuje_kolejne_komputery.html

European Network and Information Security Agency also draws attention to the inconsistency of definitions and emphasizes importance of international cooperation in the field of cyber security in the recommendations included in National Cyber Security Strategy accepted by 10 UE countries since 2008. The Agency stresses the necessity to form universal definitions which could be a base for UE countries to create national strategies supporting global cyber security.

NATO *Cooperative Cyber Defense Centre of Excellence* in Tallinn provides the definition of cyberspace as 'systems and services connected in time either directly or indirectly to the Internet, telecommunications and computer networks[4].'

Lack of consistent system and legal solutions limits the states, institutions and entities to provide global cyber security. Unrestrained by law criminals develop new forms of using cyberspace for illegal activities, which is also strengthen by dynamic changes resulting in never-ending "arms race" between criminals and groups responsible for cyber security.

The most common threats in cyberspace are:

- Malware, viruses, warms attacks;
- Theft, modification or damage of data;
- Blocking access to services (mail bomb, DoS, DDoS[5]);
- Spam;
- Phishing.

These kinds of attacks can also be legitimate to solve problems which so far were solved with conventional means and posed threat to people, e.g.: delay of the Iranian nuclear program.

Militarization of cyberspace

Cyberspace is used also by terrorists as a cyberterrorism. Many incidents attributed to terrorists can be forms of vandalism, secretly sponsored activity or activity informally accepted by the state, which is however, difficult to prove. The example of this were mass attacks on information and communication infrastructure of Estonia in 2007. The attacks paralyzed the state and blocked access to banking system and mobile telephony. Considering huge costs and possible difficulties in organizing an effective and spectacular cyber attack on well protected targets it is rather impossible for a terrorist group to take such action without government support.

Cyberspace is used for surveillance. In the report by the USA counterintelligence services chosen states (the report includes China and Russia) use cyberspace extensively to collect intelligence, especially economic data on modern technologies, defense and pharmaceutical industry.

---

[4] *National Cyber Security Strategies*, European Network and Information Security Agency, May 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cybersecurity-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport (retrieved: 23rd May 2012).

[5] (DoS) attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service (DDoS) large numbers of compromised systems attack a single target. Thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down,
thereby denying service to the system to legitimate users.
http://searchsoftwarequality.techtarget.com/definition/denial-of-service (retrieved 3 Feb. 2015).

The Internet is a source of useful information about competitors and enemies so it is rather improbable for any of global powers to damage it.

Military actions I cyberspace, called, after land, sea, air and universe, another environment of combat. International organizations as well as countries agree upon the necessity to develop defense capabilities in cyberspace. Some countries create appropriate structures in the armed forces and conduct research on new kinds of "cyberweapon" building up their own resources to deter probable adversaries. Militarization of cyberspace involves development of tools for combat in this environment.

Source: ://nt.interia.pl/internet/news-jak-usa-przygotowuja-sie-do-cyberwojny,nId,1592307

There are still a lot of llegal inconsistencies concerning combat in cyberspace. Some countries create strategies of defense and openly speak about possibility of offensive or risk of retaliation in cyberspace. The example is an American project "Olympic Games" which, according to mass media news, aimed at blocking the Iranian nuclear program.

An issue of cyperspace defense was raised in two declarations accepted after NATO Summits in 2010 and 2012. However, it is difficult to predict if a cyber attack on one of aliens would trigger mechanisms of Article 5 of the Washington Treaty[6] and what the extent of actions taken would be.

Poland and threats in cyberspace

Crime Code renewed in 2004 introduced to the Polish legislation system the provisions on cybercrime of Convention on Cybercrime signed by Poland in 2001[7]. The Crime Code

[6] Prepared in Washington on 4th April 1949 r. (J.L.2000, No. 87, p. 970).

[7] *Convention on Cybercrime, CETS No.: 185*, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=29/05/2012&CL=ENG (retrieved: 29th May 2012 r.).

includes only criminalisation of computer crimes and crimes against security of IT systems[8] without providing clear definitions.
Problem of security in cyberspace goes beyond the frames of the offensive act in a traditional understanding that in the Crime Code. In some extreme cases this act can have the form that in the light of constitutional law can constitute a reason for announcement of the state of emergency.

Source: http://gadzetomania.pl/3127,konflikt-ktorego-nie-ma-cyberzolnierze-niewidzialnej-wojny

On 27th of September 2011 the President of the Republic of Poland Bronisław Komorowski signed the amendment to the Law of War[9]. The proposal of amendment prepared in the National Security Agency introduced the term "cyberspace" to the Polish law. The accepted definition explains that cyberspace is a space for processing and exchange of information, which is created by information and communications systems, in terms of the Art. 3 p. 3 of the Law on 17th February 2005 on informatization of activity of entities fulfilling their public tasks and relationships between them and the users (J.L. No. 64, p. 565, as amended). This definition is similar to that provided by CCDCoE, as it includes technical and human elements of cyberspace.
Introduction of this definition was especially important for institutions and bodies responsible for security as it gave way to creating a set of effective instruments required to fulfill their task according to principles of legality. Accepted solutions are consistent with the Strategic Concept of NATO and constitute a part of the National Cyber Security Program (2011-2016) prepared by the Council of Ministers.

[8]After the incidents against signing ACTA by Poland (discussed in further parts of the article) the investigation was opened on the basis of Art, 269a The Penalty Code: Whoever destroys, deletes or changes a record on an electronic information carrier, having a particular significance for national defense, transport safety, operation of the government or other state authority or local government, or interferes with or prevents automatic collection and transmission of such information shall be subject to the penalty of deprivation of liberty or a term of between 3 months and 5 years. http://www.tvn24.pl/1,1737163,druk.html (retrieved: 29th May 2012).
[9]Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw, (Dz.U. 2011, Nr 222, poz. 1323).

Published on 17th April 2012 by CERT Poland[10] the annual report of 2011 includes the analysis of threats in Polish computer networks based on over 21 mln notifications about incidents from automatic systems discovered that year. In formulated findings CERT Poland Report[11] pay attention to the following facts:

- in 2011 new sources of information appeared; they contributed to better detection of computer incidents (increase by 76% compared to 2010);
- attacks on mobiles phones (smart phones) are more and more common. New version of popular Zeus Trojan, which attacks not only computers but also mobile phones appeared;
- e-banking (financial systems, confidential information) is still a target;
- significant number of incidents in 2011 automatically dealt by CERT Poland were connected with phishing (increase by 1/3 compared to 2010);
- in 2011 CERT Poland received relatively few notifications about DDoS attacks. However, it can be explained by difficulties in detecting this kind of attacks by the third party and the resistance of the victims to report this incident.

In January 2012 the series of incidents connected to security of information and communications systems of Polish state institutions took place. The attacks happened in the period from 21st to 25th January and had a form of hacktivism – an organized protest in a cyberspace against signing ACTA (Anti-Counterfeiting Trade Agreement) by Polish authorities. This document was an agreement to create new global intellectual property (IP) enforcement standards. This attack was a part of global campaign against legal changes, which – in protesters' opinion – could limit freedom of speech on the Internet.

In case of Poland a hotspot was the attack (mainly DDoS attacks) organized by hackers, who blocked access to the Internet sites of public administration institutions.

The effects of the attacks prove insufficient protection of the Internet sites under gov.pl, which are on outside servers insufficiently prepared to block massive DDoS attacks.

Conclusion

The analysis of discussed threats clearly show that Polish information recourses and elements of information and communication infrastructure are vulnerable to the same trends as the cyberspace on the global level. Along with the development of informatization of the state it is necessary to create effective solutions: preventive, technical, organizational and legal to protect citizens. The entities responsible for providing cybersecurity in Poland are: Ministry of Internal Affairs, Ministry of Administration and Digitization, Ministry of National Defense, Internal Security Agency, Military Counterintelligence Services and private sector.

Their common aim is:

[10] CERT Polska - a team operates within the structures of NASK (Research and Academic Computer Network) - a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. CERT Polska is the first Polish computer emergency response team. Active since 1996 in the response teams community, the core of the team's activity has been handling security incidents and cooperation with similar units worldwide. http://www.cert.pl/o-nas (retrieved 3rdFeb. 2015).

[11] Raport CERT Polska 2011, CERT Polska, http://www.cert.pl/PDF /Raport_CERT_Polska_2011.pdf (retrieved: 15th May 2012).

- protection of state critical information and communications infrastructure from threats from cyberspace;
- creating coherent policy on security of cyberspace for public and private sector on the state level;
- creating effective system of coordination for cooperation between public and private sector in the field of security in a cyberspace;
- controlling effects on computer incidents to minimize their costs;
- increasing social awareness of cybersecurity.

Cyberspace is a new environment for security and requires numerous changes practical as well as legal and organizational ones in global security systems. The most important then is understanding the dynamics of changes in this environment.

Bibliography

1. Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu. Michał Grzelak, Krzysztof Liedel.
2. Doktryna cyberbezpieczeństwa RP, BBN, Warszawa 22.01.2015,
3. Adamski A., Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy.
4. Bógdoł-Brzezińska A., Gawrycki M., Cyberterroryzm i problemy bezpieczeństwa informacyjne we współczesnym świecie, Wydawnictwo ASPRA-JR,
5. Polityka ochrony cyberprzestrzeni RP, MAC, Warszawa 25.06.2013 r.
6. Raport CERT Polska 2011, CERT Polska, http://cert.pl/PDF/ Raport_CERT_Polska_2011.pdf
7. Raport z działalności zespołu CERT.GOV.PL za I kwartał 2012, CERT.GOV.PL,http://cert.gov.pl/download/3/136/Raport_CERT_GOV_PL_za_I_kwartal_2012.pdf
8. Raport z działalności zespołu CERT.GOV.PL za II kwartał 2012,CERT.GOV.PLhttp://cert.gov.pl/portal/cer/56/561Raport_z_dzialalnosci_zespolu_CERTGOVPL_za_II_kwartal_2012.