M.Sc. Małgorzata BUJEK
Faculty of National Security and Logistics
Polish Air Force Academy

CYBERSECURITY AS THE BASIS FOR STATE AND SOCIETY SECURITY IN THE XXI CENTURY

Abstract

Cybersecurity is one of the most common security topics at present times. Society has enormous capabilities and possibilities in the cyberspace which create opportunities and threats as well. A cyberwar, a cyberterrorism and a cybercrime have permanently entered the catalog of threats for security. This kind of situation in a cyberspace determines need for coordinated activities at international and national level which will provide an acceptable level of security in this area.

This article presents and briefly outlines threats for the state cybersecurity. There are also presented activities aimed to lead protection of this area. In addition, author analyzed the current structure of cybersecurity system in the Republic of Poland.

Key words: cyberspace, cybersecurity, threats, cybersecurity system

Introduction

The armed struggle between states, political groups or international organizations in present times is not a typical armed struggle with use of armed forces or military formations. Currently, these activities take place in new areas which were not used in previous years. Today, conflicts are primarily a information struggle or even war in cyberspace. These kind of activities are characterized by attacks conducted by hackers on critical infrastructure or economic state potential. Threats in cyberspace does not only affected state activities but also can be cause of paralyze whole structure, offices and state institutions without use of armed forces. Such activities are not domain of criminal groups or other organizations which are geared to steal information or gain only economic profits. Currently, these activities are also being undertaken by states. A good example is South Korea which has a hacker specialized military units constantly trained and ready to use any time.

It is also well known that China leads cyber war with the US. There is a very good example which occurred between April and May in 2007 in Estonia. Government servers, national websites, banks, suppliers of telecommunications services were paralyzed due to cyber attack which threatens security of state[1].

Therefore, protection of cyberspace tends to be one of key areas of safety. Without a doubt, stable functioning and development of the global information society depends on an open, reliable and secure cyberspace[2].

The concept of cyber security, division and characterization of threats connected to this area

The area of cybersecurity is horizontal, it permeates all sectors of the state economy and affects activity of the state and society in almost all its dimensions[3]. Unfortunately, the current difficulties with a coherent definition of terms connected to cybersecurity are one of the biggest obstacles to make formal and legal regulation of cybersecurity at national and international level as well. It is important to establish definition of terms connected to cybersecurity around which, there will be develop national strategies by states. These activities will help to maintain a proper global level of cybersecurity.

In case of cybersecurity concept, there is not defined a single definition of this term. According to *Doktryna cyberbezpieczeństwa RP* signed in 2015 the cybersecurity term means *the process of ensuring safe operation of the state in the cyberspace as its whole structures, individual and legal persons together with entrepreneurs and other non-legal entities, as well as IT systems and information resources in the global cyberspace*[4]. This document presents official views and arrangements for purposes, environmental assessments and concepts (principles and methods) of activities (including good practices) to ensure safe operation of the state, its individuals and legal entities - including entrepreneurs and other entities in the cyberspace.

There is other important document related to this subject called *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* adopted by resolution of the Council of Ministers on 25 June 2013. There were discussed, among others, issues of combating cybercrime, identify the competent authorities to increase the level of cybersecurity and finally

[1]A. Polak, P. Paździorek (red.), *Siły i środki walki zbrojnej w wojnach przyszłości*, AON, Warszawa 2016, p. 130-131.
[2]Ibidem, p. 130-131..
[3] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego 9/13, p. 225.
[4] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, p. 8-9.

cooperation between private and public sectors for security of whole cyberspace. According to this document, cyberspace security is defined as *set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace*[5].

In accordance to *Doktryna cyberbezpieczeństwa RP* signed in 2015, cyberspace is defined as *space of processing and exchange of information created by the ICT systems (teams of interoperable IT equipment and software which provide processing, storage, also sending and receiving data over telecommunication networks by means of a device appropriate for specific type of telecommunication network which is intended to direct or indirect connection to the network terminals) together with links between them and the relations with users*[6].

One of the best known and most widely quoted is the definition of the cyberspace formulated by the US Department of Defense. It was done for created dictionary of military and associated terms. According to mentioned document, this term is understood as: *A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*[7].

Together with technology development, it is possible to find counterparts in cyberspace for all traditional internal threats for security. It is done by the fact that cyberspace gives opportunity to achieve results at relatively low cost. In present times, it is not necessary to use expensive missiles, bombs and tanks to deprive states of access to electricity or disrupt operation of transport. Cheaper ICT tools can be used successfully by state and non-state entities as well. As we can see, cyberattack has become a very attractive tool for asymmetric conflicts due to fact that it is possible for a weaker entity to neutralize opponent predominance. Undoubtedly, cyberspace often and often becomes a scene of very intense espionage activities aimed at obtaining state secrets and business information. According to reports of companies dealing with IT security, the aim of network espionage activities are government administration institutions and key companies for energy sector from point of view of the polish economy. The loss of the most secure information means weakening of the state's potential in the most important areas of its functioning. What is more, it is possible that real effects of carried out attacks can be noticed in the future. It means,

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, p. 5.
[6] *Doktryna cyberbezpieczeństwa*…, p. 7.
[7] *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 February 2016), p. 58.

effect will be noticed when the aggressor decides about that[8]. Important is that actions in cyberspace often remain anonymous because it is very difficult to determine exactly who is responsible for them. The aggressor can intercept computers of uninformed users and use them to create a global network for aggressive cyberattacks.

Among others cyberterrorism, cybercrime, cyberespionage, hysteria and haccaratism are major threats for cyberspace in present times.

The scope of cyber terrorist threats is very wide. These are a global phenomenon which take very different forms of action. Effective prevention before this phenomenon requires careful identification of threats in this area and creation counter strategies. Up to now there is no one universally recognized definition of cyberterrorism concept. Most often it is defined as a politically motivated attack on information systems (software) or computers and networks (hardware). The main purpose of these attacks is to destroy infrastructure, intimidate the population and force the government to take specific actions. Cyberterrorism takes many forms for example disturbance of functioning the Internet and information systems of critical infrastructure or taking control of telecommunication networks[9].

Cybercrime can be defined in many different ways. Among others, it is described as a type of economic crime in which the computer is either a tool or object of a crime. Cybercrime can be considered as sub-category of computer crime. This term defines all types of offenses committed by the Internet or other computer networks. There is no one universal definition up to now. The Council of Europe Convention on Cybercrime signed in Budapest in 2001, specifies that elements of this phenomenon are: widely understood security breaches (such as haking, illegal obtaining of data), fraud and forgery and copyright infringement as well[10]. In addition, there are also counted to cybercrimes:

- cyberintrusions – criminals has received unauthorized access to data from a computer or network without criminal use or destruction of data. Cyberintrusion also is identified with hacking which is described in next part of article,
- cybertheft – this is use of computer or network to take advantage of someone else's property. Specific types of cybertheft include embezzlement, unauthorized

[8] http://www.rp.pl/Rzecz-o-prawie/312269987-Cyberbezpieczenstwo-to-strategiczne-wyzwanie-dla-panstwa.html #ap-1, access: 11.04.2017.

[9] K. Liedel, P. Piasecka, Wojna cybernertyczna-wyzwanie XXI wieku, [in:] Bezpieczeństwo Narodowe, I-2011/17, Wyd. BBN, Warszawa 2011, p. 18.

[10] *Konwencja Rady Europy o Cyberprzestępczości*, Rada Europy, Budapeszt, 23.11.2001.

misappropriation, corporate espionage (industrial), plagiarism, computer piracy or identity theft[11].

- cyberdestruction – this is a crime in which network services are interrupted and data is destroyed or deleted rather than stolen. As an example it can be mentioned: hacking into a server or web page and then injecting malicious software[12].

In case of cyberespionage, it is defined as illegal acquisition of classified information. It is an intelligence method which is very comfortable, effective and difficult to detect. Classified information is obtained by weakening or bypassing access control mechanisms and intrusion into protected systems as well[13]. Loss of this kind of information may pose a serious security risk. Cyberespionage is characterized by other methods than cyberterrorism. There are used more advanced techniques to provide anonymity (it is important to remember that nowadays special groups and government interviews use such means of obtaining information at present times).

Nowadays, hacking and hysteria become more and more popular. Hacking is the oldest and the most popular form of use computer security vulnerabilities. This is nothing more than the use of telecommunications equipment to gain unauthorized access to the computer system. It is also defined as a classic form of an assault on the electronic security of processed information[14]. Initially, hackers who broke electronic protection of computer systems were not considered as a significant threat. The situation was changed at turn of the 80s and 90s of XX century. There were incidents which have become more and more widespread not only to check security but also to find gaps for criminal or political purposes[15].

Hactizm is a combination of activism and criminal activity. It uses hacking methods against specific targets on the Internet. It interferes operation but does not cause any serious damages. This activity is not intended to destroy the opponent's resources but to focus on some problem[16]. Hactista is a person who use his superior computer skills to promote certain political demands. Hactizm is different than hacking. Hactizm is dedicated to propagate attitudes or political protests on a very large scale. Hacticism has grown in strength

---

[11] B. Hołtys, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo 1, 2011, p. 18.
[12] Ibidem.
[13] D. Krawczyk, *Internet zagrożeniem bezpieczeństwa wewnętrznego*, Horyzonty Bezpieczeństwa, No. 2(1) 2016.
[14] Ibidem.
[15] M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw*, p. 51-52; R. Trigaux, *A History of Hacking*, „St. Petersburg Times Online", http://www.sptimes.com/Hackers/history.hacking.html, 07.05.2017.
[16] K. Liedel, P. Piasecka, *Wojna cybernertyczna-wyzwanie*…, p.18.

at the beginning of the XXI century due to the Anonymous group. This group has made many high-profile actions on the Internet in recent years aimed to focus on the world's attention to its postulates. People who use hactizm often acquire confidential information and block specific services to achieve propaganda purposes.

Use of cyberspace for military operations

Consideration about possibility to lead a war in the Internet started together with development of computerization and growth progress of technology. It was very soon realized that use of cyberspace in armed conflict is very effective. Initial attempts were made during Operation Desert Storm and than in Chechnya[17]. Cyberspace has become a well field clashes for Serbian and NATO intelligence officers during the North Atlantic Alliance interventions in Kosovo in 1999. Initially these operations were simple. It was not caused by lack or little experience in this area but rather by an attempt to hide all abilities and means use in operations (for example limited US intervention in Iraq in 2003). The White House did not decide to use full potential to attack the Iraqi critical infrastructure at that time due to fear of hard to foresee legal consequences and aversion to disclosure new technology to future opponents[18]. The breakthrough in this issue occurred in 2007. As it was mentioned before, there were mass cyberattacks in Estonia which were referred as "the first cyberwar" although these activities were not military. These cyberattacks contributed to the perception of this problem by the international public. Only a few months later, Israeli used its potential in this area during Orchard operation which was aimed to destroy the nuclear weapons research center in Syria. Because of that, there was infected the Syrian air defense system and Syrian soldiers had not possibility to detect Israeli aircraft as a result[19]. However not all attacks are related to real destruction, for example critical infrastructure. The attack can also be targeted at servers or military networks. Therefore, it should be remember that the military use of cyberspace has various methods and forms. The main purpose of such attacks is to perform military tasks which strike into different dimensions of life. Because of that, it is possible to identify military attacks with use of cyberspace as those which are supposed to support or replace traditional warfare.

According to analyze of all methods to attack on network, it is possible to make conclusions like that: evolution of the battlefield and its character together with rapidly

[17] F. Schreier, On Cyberwarfare, „DCAF Horizon 2015 Working Paper", vol. 7, p. 107.
[18] M. Lakomy, *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, [in:] *e-Politikon* nr 6/2013, p. 104
[19] Ibidem, p. 132.

changing phenomena which determine attacks are indicators of the state approach to national and international security. Change of the conflict area to cyberspace has become a reality in the XXI century. Any changes associated with it have a real impact on the creation and analysis of national policies and strategies creation of the most effective cybersecurity system in each state.

Activities aimed to protect cyberspace of the Republic of Poland

Cyberspace is a wide area which includes all sectors of the national economy and thus it has an influence on the functioning of the state and society. For this reason, it is necessary to develop a system aimed to ensure security in national sphere. The activities leading to the protection of cyberspace should be part of the constitutional order of the state. The Polish cybersecurity system should be based on cooperation between its components. The aim of this cooperation will be to detect, prevent and counter potential attacks as well. Continuous cooperation and coordination are necessary to minimize the negative effects which could occur in relation to national IT systems. The effectiveness of activities is largely dependent on efficiency of the risk management process. Therefore, it is necessary to provide[20]:

- single methodology for risk assessment,
- conduct database which contain information about identified vulnerabilities,
- determine limits for risk levels at each level of cybersecurity system hierarchy.

The purpose of the risk management process is nothing more than assessment of probability of threats occurrence and reduction risk level to acceptable.

The current cybersecurity system consists of the Ministry of Defence, the Government Security Centre, the Ministry of Digitization, the Council of Ministers, the Internal Security Agency, the Police Headquarters, the Ministry of Justice, the Office of Electronic Communications and CERT Poland[21,22]. The Ministry of Defence is responsible for the military zone of cyberspace protection. The Government Security Centre holds a leading role in the field of crisis management and critical infrastructure protection, moreover, there

[20] *Strategia Cyberpbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 12.
[21] CERT (Computer Emergency Response Team) – this name is reserved by Carnegie Mellon University and its use requires approval of the university. This consent has CERT Poland. Directive NIS uses name CSIRT (Source: *Strategia Cyberpbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 16).
[22] *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 4.

is service on duty responsible for transmission of information about the dangers in field of crisis management. The Ministry of Digitization, in simple words, is the strategic and political coordinator in protection of cyberspace. In addition, this institution in cooperation with the Internal Security Agency developed following document: *Polityka Ochrony Cyberprzestrzeni RP*. Important role is realized also by the Internal Security Agency which domain is protection before violations against internal security of the state and citizens. The Police is responsible for combating cybercrimes. The last one, means CERT Poland is in charge of registration activities which violate cybersecurity, alert about occurrence of threats for network users, test of products in the field of IT security and increase awareness related to discussed issues.

The actual measures connected with protecting cyberspace of the Republic of Poland have unorganized nature. This is due to imitating foreign experiences[23]. In addition, there is still not developed the law related to considered problems. For this reason, it is necessary to take initiatives to introduce coordinated procedures aimed to counter threats which appear in cyberspace. Important is also to establish a single supervisory body which will oversee activities of other elements included in the presented security system. To achieve this assumption it is essential to initially created a map of entities which will be a part of cyber security model. During the next step, there should be consider possible variants, specification of tasks and responsibilities of various components[24].

Combating cybercrime requires knowledge of criminals motives and applied technical solutions. In addition, it is necessary to find evidence of committing criminal acts. Very important is to develop and implement the model to combat this type of acts. One of the proposals was presented by J. Kosiński. It consists of three phases. The first one (investigation network) based on the assertion of committing a crime, identify evidence, the place where crime was committed and the suspect or the perpetrator. The second phase - management of the crime place is nothing more than collection of digital evidence and arrest the suspect as well. The last phase, called analysis of digital evidence, is to restore course of events, indication of used tools and possible accomplices. In addition, J. Kosiński proposes to use a specific structure of a unit responsible for combating cybercrimes. The structure is as follow[25]:

[23] *Założenia strategii …*, p. 4.
[24] *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015, p. 69.
[25] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin SA, Warszawa 2015, p. 214-215.

- the operational and investigative team which is responsible for monitoring the network, and to say more specifically, conducting operational and reconnaissance activities,
- the reactive and investigative team which performs tasks consists of finding devices used to crimes and then secures traces and typing of suspects,
- the forensic laboratory is to study secured traces and verifying forensic hypotheses,
- the research and development group develops models of crimes in cyberspace, conducts trainings and creates tools which are necessary to work.

Extremely important in activities of discussed unit to combat cybercrimes is to exchange information between teams.

Ensuring security in cyberspace is not possible without proper legislation. For this reason, there are proceeding works connected to preparation the law draft of the national cybersecurity system. This is due to the need to introduce solutions to create a basis for effective system to protect information resources of all public, businesses entities and citizens. The aim of the law is to create system of protection IT architecture at the national level together with respecting international rules and establish system to respond on threats in considered area[26].

To protect cyberspace, there is also important cooperation between public administration entities and other bodies performing a significant role in cyberspace. It should be taken into account the proceedings nature of such a large group of stakeholders as it is possible. Among others, there could be mention[27]:

- telecom operators,
- security solution providers.
- social media,
- entrepreneurs who are part of the critical infrastructure and many others.

In order to counter threats in cyberspace it is important to manage IT resources and infrastructure for collection and processing data in systemic way. This is possible due to, for example definition of objectives and rules of conduct, continuous identification and analysis of existing threats, determining possible security measures and implementation of training programs.

---

[26] http://bip.kprm.gov.pl/kpr/wykaz/r2225,Projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa.html, access: 19.01.2017 r.

[27] *System bezpieczeństwa*…, p. 157.

In terms of information and communication security at the national level, it is necessary to establish agreements and coordination of common multinational activities. Therefore, one of the goals of Polish policy is to refer as much as possible benefits in activity in this sphere[28]. Representatives of the Republic of Poland should strengthen position of the state at international arena. Because of that, there should be created a single way of cooperation at national and international level.

It is important to point currently developed document *Multinational Defensive Cyber Operations* – MDCO. This is a guide intended to be an attempt to limit risk of hazards and indicate directions of conduct for protection cyberspace. There are no standardized framework for international combined efforts at this time. MDCO is to create basis for preparation of joint operations for protection cyberspace, for example by developing a single system of collecting information. The document focuses on five elements needed in forming Multinational Defensive Cyber Operations. These are: Authorities, Intelligence and Cyber Key Terrain, Risk Assessment and Risk Management, MDCO Capabilities, Cyber Command and Control Organization.

Particularly noteworthy are the last two parts. The chapter MDCO Capabilities include information concerning possibility of detect, analyze, counter and also reduce likelihood of risks and vulnerabilities in the system of cyberspace as well. It should be understood as passive and active measures taken in course of multinational efforts to protect data and networks. The last section of this document (Cyber Command and Control Organization) has been devoted to determine authority at the national level responsible for operations in cyberspace and means used in operations.

Conclusion

Cyberspace phenomena and processes have a huge impact at national and international security as well. Modern technologies are rapidly develop and together with that there are develop threats for cyberspace. It is important to analyze methods and measures use by cyberterrorists and cybercriminals. It is also important to prepare for future threats and challenges. Cyberterrorism is considered as a serious threat for public order, security and also for standards by which democratic societies are organized. It is usually politically motivated. Its effect is to use violence against non-combatants targets by transnational groups or secret agents. All entities which operate on the Internet, perform tasks and addict

[28] *Strategia Cyberpbezpieczeństwa…*, p. 24.

effectiveness of any aspect of operation from network or storage and sharing resources should responsibly treat IT and ICT security issues. Private entrepreneurs, households, offices, banks, government units, ordinary users and every person can become victim of cybercriminals. Cyberthreats are a global challenge. It is important to coherent and complementary approach to develop mechanisms to counter these threats which are placed in cyberspace. Specialists from the Organization for Security and Co-operation in Europe appeal for international legislation to prevent cyber criminals from triggering an international crisis. There are estimated $ 100 billion per year losses caused by cybercrimes.

Due to complexity of this issue, there are only outlines of topics related to cyberspace and cybercrimes in the article. It is require to conduct extensive theoretical and empirical research to make a precise analyze of these problems.

Bibliography

1. Hołtys B., Pomykała J., *Cyberprzestępczość,ochrona informacji i kryptologia*, Prokuratura i Prawo 1, Warszawa 2011.
2. Kosiński J., *Paradygmaty cyberprzestępczości*, Wyd. Dyfin SA, Warszawa 2015.
3. Krawczyk D., *Internet zagrożeniem bezpieczeństwa wewnętrznego*, Horyzonty Bezpieczeństwa, nr 2 (1) 2016.
4. Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, e-Politikon, nr 6/2013.
5. Lakomy M., *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw*, R. Trigaux, A History of Hacking, St. Petersburg Times Online, [dostęp 07.05.2017].
6. Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, [w]: Bezpieczeństwo Narodowe, I-2011/12, Wyd. BBN, Warszawa 2011.
7. Polak A., Paździorek P. (red.), *Siły i środki walki zbrojnej w wojnach przyszłości*, Wyd. Akademii Obrony Narodowej, Warszawa 2016.
8. Schreier F., *On Cyberwarfare*, DCAF Horizon 2015 Working Paper, vol. 7.
9. Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, Przegląd Bezpieczeństwa Wewnętrznego, nr 9 (5) 2013.
10. *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 February 2016).
11. *Doktryna cyberbezpieczeństwa RP*, Warszawa 2015.
12. *Konwencja Rady Europy o Cyberprzestępczości*, Budapeszt 2001.

13. *Strategia Cyberbezpieczeństwa RP na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa 2016.
14. *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015.
15. *Polityka Ochrony Cyberprzestrzeni RP*, Warszawa 2013.
16. *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016.
17. Baryłka A., *Wprowadzenie do zagadnienia obronności i bezpieczeństwa w planowaniu i zagospodarowaniu przestrzennym.* Aparatura Badawcza i Dydaktyczna nr 3/2016.
18. http://bip.kprm.gov.pl/kpr/wykaz/r2225,Projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa.html.
19. http://www.rp.pl/Rzecz-o-prawie/312269987-Cyberbezpieczenstwo-to-strategiczne-wyzwanie-dla-panstwa.html#ap-1.