CYBERSECURITY AS THE BASIS FOR STATE AND SOCIETY SECURITY IN THE 21ST CENTURY

Małgorzata BUJEK, M.A.
National Security and Logistics Faculty
Polish Air Force Academy
ul. Dywizjonu 303 no 35
08-521 Dęblin, Poland
m.bujek@wsosp.pl

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, cyberterrorism and cybercrime have permanently entered the catalog of threats for security. This kind of situation in a cyberspace determines the 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 provide protection in this area. In addition, the author analyzed the current structure of the cybersecurity system in the Republic of Poland.

Keywords: 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 the 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 an information struggle or even wars in cyberspace. These kinds of activities are characterized by attacks conducted by hackers on critical infrastructure or economic state potential. Threats in cyberspace do not only affect state activities but can also cause the paralysis of the whole structure, offices and state institutions without the use of armed forces. Such activities are not a domain of criminal groups or other organizations which are geared to steal information or gain merely an economic profits. Currently, these activities are also being undertaken by states. A good example is South Korea which has hacker specialized military units constantly trained and ready to use at any time. It is also well known that China leads a cyber-war with the US. There is a very good example supporting the claim that cyber-wars are waged, namely the situation that occurred in Estonia in April and May of 2007. The government servers, national websites, banks, suppliers of telecommunications services were paralyzed due to a cyber-attack which threatened the security of the state[1].

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

THE CONCEPT OF CYBER SECURITY, CLASSIFICATION AND CHARACTERISTICS OF THE THREATS RELATED TO THIS AREA

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

In case of the cybersecurity concept, there is no single definition of this term. According to the cybersecurity doctrine of the Republic of Poland [*Doktryna cyberbezpieczeństwa RP*] signed in 2015, "cybersecurity" means "the process of ensuring safe functioning in cyberspace of the state as a whole, its structures, natural and legal persons, including entrepreneurs and other non-legal entities, as well as IT systems and information resources of the global cyberspace they use"[4] (own transl.). This document presents official views and arrangements regarding the 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.

[1] A. Polak, P. Paździorek (ed.), *Siły i środki walki zbrojnej w wojnach przyszłości*, AON, Warszawa 2016, pp. 130-131.

[2] A. Polak, P. Paździorek (ed.), *Siły i środki walki zbrojnej w wojnach przyszłości*, AON, Warszawa 2016, pp. 130-131.

[3] J. Wasilewski, „Zarys definicyjny cyberprzestrzeni", *Przegląd Bezpieczeństwa Wewnętrznego* 9/13, p. 225.

[4] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, pp. 8-9.

There is another important document related to this subject called *The Cyberspace Policy of the Republic of Poland* (*Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*) adopted by resolution of the Council of Ministers on June 25, 2013. There were discussed there, among others, the issues of combating cybercrime, the procedures of identifying competent authorities to increase the level of cybersecurity, and finally the cooperation between private and public sectors for security of the whole cyberspace. According to this document, cyberspace security is defined as "a set of organizational and legal, technical, physical and educational projects aimed at ensuring the uninterrupted functioning of cyberspace"[5].

In accordance to the cybersecurity doctrine of the Republic of Poland (*Doktryna cyberbezpieczeństwa RP*), signed in 2015, cyberspace is defined as "the space of processing and exchanging information created by the ICT systems (sets of interoperable IT equipment and software, which facilitate data processing, their storage, as well as sending and receiving through telecommunication networks by means of a device appropriate for a specific type of telecommunication network which can be directly or indirectly connected to interfaces) together with the links between them, and the relations with users" (own transl.)[6].

One of the best known and most widely quoted is the cyberspace definition formulated by the US Department of Defense. It was created for the dictionary of military and associated terms. According to that 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].

As the technological development progresses, it is possible to find counterparts in cyberspace for all traditional internal threats for security. It is due the fact that cyberspace gives an opportunity to achieve results at relatively low cost. Nowadays it is not necessary to use expensive missiles, bombs and tanks to deprive states of the access to electricity or disrupt the 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's predominance. Undoubtedly, cyberspace more and more often becomes a scene of very intense espionage activities aimed at obtaining state secrets and business information. According to the reports of companies dealing with IT security, the aim of the network espionage activities are government administration institutions and key, from the point of view of the Polish economy, energy sector companies. The loss of the most secure information means weakening the state's potential in the most important areas of its functioning. Moreover, it is possible that real effects of carried out attacks can be noticed in the future. It means that the result of the attack can be noticed only when the aggressor decides that[8]. What is also 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 hacking are major threats for cyberspace today.

The scope of cyber terrorist threats is very wide. They are a global phenomenon that takes very different forms of action. Effective prevention against it requires careful identification of threats and creating proper counter strategies. Up to now there is no one universally recognized definition of cyberterrorism. 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 a disruption of functioning of the Internet and information systems of critical infrastructure or taking control over telecommunication networks[9].

Cybercrime can be defined in many different ways. It may be 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 through the Internet or other computer networks. The Council of Europe Convention on Cybercrime signed in Budapest in 2001 specifies the elements of the phenomenon: widely understood security breaches (such as hacking, illegal obtaining of data), fraud and forgery and copyright infringement[10]. In addition, the following offenses are also counted as cybercrimes:

- cyber-intrusions – criminals have received unauthorized access to data from a computer or network without a criminal use or destruction of data; cyber-intrusion also is identified with hacking which is described later on in this article,
- cyber-theft – this is a use of computer or network to take advantage of someone else's property; specific types of cyber-theft include embezzlement, unauthorized misappropriation, corporate espionage (industrial), plagiarism, computer piracy or identity theft[11].

[5] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, p. 5.

[6] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Warszawa 2015, p. 7.

[7] *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 February 2016), p. 58.

[8] J. Świątkowska, "Cyberbezpieczeństwo to strategiczne wyzwanie dla państwa", *Rzeczpospolita* 26.12.2015, retrieved from: http://www.rp.pl/Rzecz-o-prawie/312269987-Cyberbezpieczenstwo-to-strategiczne-wyzwanie-dla-panstwa.html, (24.10.2017).

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

[10] *The Council of Europe Convention on Cybercrime*, The Council of Europe, Budapest, 23.11.2001.

[11] B. Hołtys, J. Pomykała, „Cyberprzestępczość, ochrona informacji i kryptologia", *Prokuratura i Prawo* 1, 2011, p. 18.

- cyber-destruction – this is a crime in which network services are interrupted and data is destroyed or deleted rather than stolen; hacking into a server or web page and then injecting malicious software can serve as an its example[12].

Cyberespionage 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[13]. A loss of this kind of information may pose a serious security risk. Cyberespionage is characterized by other methods than cyberterrorism. More advanced techniques are used to secure anonymity (it is important to remember that nowadays special groups and governments use such means of obtaining information).

Hacking and hysteria become more and more popular these days. Hacking is the oldest and the most popular form of use computer security vulnerabilities. This is nothing more than a 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 1980s and 1990s. There were incidents which have become more and more widespread and were undertaken not only to check security but also to find gaps for criminal or political purposes[15].

Hacktivism is a combination of activism and criminal activity. It uses hacking methods against specific targets on the Internet. It interferes the operation but does not cause any serious damages. This activity is not intended to destroy the opponent’s resources but to turn attention to a certain problem[16]. A hacktivist is a person who uses their superior computer skills to promote particular political demands. Hacktivism is different than hacking. Hacktivism is dedicated to propagate attitudes or political protests on a very large scale. It grew in strength at the beginning of the 21st century due to the Anonymous group. This group has made many high-profile actions on the Internet in recent years that aimed turn the world’s attention to its postulates. People who use hacktivism often acquire confidential information and block specific services to achieve propaganda purposes.

USE OF CYBERSPACE FOR MILITARY OPERATIONS

Considerations about the possibility to wage a war in the Internet started together with the development of computerization and the growing progress of technology. Quite soon people realized that the use of cyberspace in armed conflict is very effective. Initial attempts were made during Operation Desert Storm and then in Chechnya[17]. Cyberspace has become a field of clashes between 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 the lack or little experience in this area, but rather by an attempt to hide all abilities and means used in the operations (for example limited US intervention in Iraq in 2003). The White House did not decide to use its full potential to attack the Iraqi critical infrastructure at that time due to fear of difficult 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 to 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, Israel used its potential in this area during the Orchard operation which aim was to destroy the nuclear weapons research center in Syria. For this purpose the Syrian air defense system was infected, and in result Syrian soldiers had not possibility to detect Israeli aircraft[19]. However not all attacks are related to real destruction of, for example critical infrastructure. The attack can also be targeted at servers or military networks. Therefore, it should be remembered that the military use of cyberspace has various methods and forms. The main purpose of such attacks is to perform military tasks which strike at different dimensions of life. Therefore, it is possible to identify military attacks with use of cyberspace as ones that are supposed to support or replace traditional warfare.

According to an analysis of all methods of the attack on networks, it is possible to draw a conclusion that evolution of the battlefield and its character, together with rapidly 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 21st century. Any changes associated with it have a real impact on the creation and analysis of national policies and strategies regarding the most effective cybersecurity system in each state.

[12] B. Hołtys, J. Pomykała, „Cyberprzestępczość, ochrona informacji i kryptologia”, *Prokuratura i Prawo* 1, 2011, p. 18.

[13] D. Krawczyk, „Internet zagrożeniem bezpieczeństwa wewnętrznego”, *Horyzonty Bezpieczeństwa* 2(1), 2016.

[14] D. Krawczyk, „Internet zagrożeniem bezpieczeństwa wewnętrznego”, *Horyzonty Bezpieczeństwa* 2(1), 2016.

[15] M. Lakomy, „Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku”, Stosunki Międzynarodowe – *International Relations* 3-4, 2010. pp. 51-52; R. Trigaux, “A History of Hacking”, *St. Petersburg Times Online*, retrieved from: http://www.sptimes.com/Hackers/history.hacking.html, (23.10.2017).

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

[17] F. Schreier, “On Cyberwarfare”, *DCAF Horizon 2015 Working Paper* 7, p. 107.

[18] M. Lakomy, „Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii”, *e-Politikon* 6/2013, p. 104

[19] M. Lakomy, „Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii”, e-Politikon 6/2013, p. 132.

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

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

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

The current cybersecurity system consists of the Ministry of Defense, 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]. The Ministry of Defense is responsible for the military part of cyberspace protection. The Government Security Centre holds a leading role in the field of crisis management and critical infrastructure protection. Moreover, there is service on duty responsible for transmission of information about the dangers in the field of crisis management. The Ministry of Digitization, in simple words, is the strategic and political coordinator of protection of cyberspace. In addition, this institution, in cooperation with the Internal Security Agency, developed following a document *Cyberspace Policy of the Republic of Poland* (*Polityka Ochrony Cyberprzestrzeni RP*). An important role is carried out by the Internal Security Agency which domain is the protection against violations of the state's internal security and the citizens. The Police is responsible for combating cybercrimes. The last body, i.e. CERT Poland is in charge of registration activities which violate cybersecurity, alerting if threats for network users occur, testing products in the field of IT security, and increasing awareness related to the discussed issues.

The actual measures to protect the cyberspace of the Republic of Poland are unorganized. This is due to an attempt to imitate foreign experiences[22]. In addition, there is still no the law related to the considered problems. For this reason, it is necessary to take initiatives to introduce coordinated procedures aimed to counter threats which appear in cyberspace. It is also important to establish a single supervisory body which would oversee the activities of other elements of the actual security system. To achieve this goal it is essential to create a map of entities which will be a part of the cyber security model. During the next step, various possible variants, specification of tasks and responsibilities of various components should be considered[23].

Combating cybercrime requires knowledge of the criminals' motives and applicable technical solutions. Moreover, it is necessary to find evidence of committing criminal acts. Developing and implementation of the model to combat this type of acts is crucial. One of the proposals was presented by J. Kosiński. It consists of three phases. The first one (investigation network) is based on the assertion of committing a crime, identification of the evidence, the place where the crime was committed, and the suspect or the perpetrator. The second phase – the management of the crime place is nothing more than a collection of digital evidence, and finally the arrest the suspect. The last phase, called "analysis of digital evidence," is to restore the course of events, indicate the used tools and possible accomplices. In addition, J. Kosiński proposes a specific structure for the unit responsible for combating cybercrimes. The structure is as follows[24]:

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

An extremely important part of such combating cybercrimes teams' work is to exchange information between teams.

Ensuring security in cyberspace is not possible without proper legislation. It is why the work has been conducted to prepare a legal draft of the national cybersecurity system. This is due to the need to introduce solutions to create a basis for effective system to protect the information resources of all the society, businesses entities, and citizens. The aim of the law is to create a system protecting the IT architecture at the national level in accordance with

[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); *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 4.

[22] *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 4.

[23] *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015, p. 69.

[24] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin SA, Warszawa 2015, pp. 214-215.

respecting international rules, and to establish a system responding to threats[25].

In order to protect cyberspace, a cooperation between public administration entities and other bodies performing a significant role in cyberspace has to be introduced. As many stakeholders should be included in the process as possible. Among those one may enlist[26]:

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

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

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 the Polish policy is to transfer resources, as much as possible, into this sphere[27]. The representatives of the Republic of Poland should strengthen the position of the state at the international arena. That is why a single way of cooperation at national and international level should be created.

It is important to point out at the 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 cyberspace protection. There is no standardized framework for internationally combined efforts at the moment. The purpose of MDCO is to create a basis for preparation of joint operations for cyberspace protection, for example by developing a single system of collecting information. The document focuses on five elements needed in forming multinational defensive against cyber operations. These are: (1) authorities, (2) intelligence and cyber key terrain, (3) risk assessment and risk management, (4) MDCO capabilities, and (5) cyber command and control organization.

Especially the last two parts are noteworthy. The MDCO Capabilities chapter includes information concerning the possibility of detect, analyze, counter, and also reduce the likelihood of risks and vulnerabilities in the system of cyberspace. 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 the authority at the national level responsible for operations in cyberspace and means used in operations.

CONCLUSION

Cyberspace phenomena and processes have a huge impact on national and international security. Modern technologies are rapidly developing and is accompanied with the growing number of threats for cyberspace. It is important to analyze methods and measures used 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 all sorts of tasks and that is why network, storage, and sharing resources should be responsibly treated and IT and ICT security measures undertaken. Private entrepreneurs, households, offices, banks, government units, ordinary users and every person can become a victim of cybercriminals. Cyberthreats are a global challenge. It is important to come up with a coherent and complementary approach to develop mechanisms to counter the cyberspace threats. 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, this article presents only an outline of topics related to cyberspace and cybercrimes. Conducting an extensive theoretical and empirical research to make a precise analysis of these problems is highly needed.

BIBLIOGRAPHY

1. *Convention on Cybercrime*, The Council of Europe, Budapest, 23.11.2001, retrieved from: https://rm.coe.int/1680081561, (24.10.2017).
2. *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 (As Amended Through 15 February 2016), retrieved from: https://fas.org/irp/doddir/dod/jp1_02.pdf, (23.10.2017).
3. *Doktryna cyberbezpieczeństwa RP*, Warszawa 2015, retrieved from: http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf, (23.10.2017).
4. Hołtys, B., Pomykała, J., Cyberprzestępczość,ochrona informacji i kryptologia, *Prokuratura i Prawo* 1, Warszawa 2011.
5. Kosiński, J., *Paradygmaty cyberprzestępczości*, Dyfin SA, Warszawa 2015.
6. Krawczyk, D., Internet zagrożeniem bezpieczeństwa wewnętrznego, *Horyzonty Bezpieczeństwa* 2(1), 2016.
7. Lakomy, M., Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii, *e-Politikon* 6, 2013.
8. Lakomy, M., Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku,

[25] *Projekt ustawy o krajowym systemie cyberbezpieczeństwa*, Biuletyn Informacji Publicznej, retrieved from: http://bip.kprm.gov.pl/kpr/wykaz/r2225,Projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa.html, (23.10.2017).

[26] *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015, p.157.

[27] *Strategia Cyberpbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa 2016, p. 24.

Stosunki Międzynarodowe – International Relations 3-4, 2010.

9. Liedel, K., Piasecka, P., Wojna cybernetyczna – wyzwanie XXI wieku, *Bezpieczeństwo Narodowe* I-2011/12, BBN, Warszawa 2011.
10. Polak, A., Paździorek, P. (eds.), *Siły i środki walki zbrojnej w wojnach przyszłości*, AON, Warszawa 2016.
11. *Polityka Ochrony Cyberprzestrzeni RP*, Warszawa 2013.
12. *Projektustawyokrajowymsystemiecyberbezpieczeństwa*, Biuletyn Informacji Publicznej, retrieved from: http://bip.kprm.gov.pl/kpr/wykaz/r2225,Projekt-ustawy-o-krajowym-systemie-cyberbezpieczenstwa.html, (23.10.2017).
13. Schreier, F., On Cyberwarfare, *DCAF Horizon 2015 Working Paper* 7.
14. *Strategia Cyberbezpieczeństwa RP na lata 2016-2020*, Ministerstwo Cyfryzacji, Warszawa 2016.
15. *System bezpieczeństwa cyberprzestrzeni RP*, Warszawa 2015.
16. Świątkowska, J., Cyberbezpieczeństwo to strategiczne wyzwanie dla państwa, *Rzeczpospolita* 26.12.2015, retrieved from: http://www.rp.pl/Rzecz-o-prawie/312269987-Cyberbezpieczenstwo-to-strategiczne-wyzwanie-dla-panstwa.html, (24.10.2017).
17. Trigaux, R., A History of Hacking, *St. Petersburg Times Online*, retrieved from: http://www.sptimes.com/Hackers/history.hacking.html, (23.10.2017).
18. Wasilewski, J., Zarys definicyjny cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego* 9(5), 2013.
19. *Założenia strategii cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*, Ministerstwo Cyfryzacji, Warszawa 2016.