Emilia Chronowska*

Selected security threats in cyberspace

Abstract

This article presents selected cybersecurity threats, identifies them, and points out their evolving nature. Cyberspace is a realm without defined geographic or political boundaries and is highly interactive. This article indicates the important role of cybersecurity in the context of building the information society and presents the most important legal regulations, both international and national, along with the indication of the proposed directions of changes at the national level, which would help to increase cybersecurity. The article emphasizes the importance of legislative and organizational regulations in the field of the addressed issues.

Key words: security, threats, cyberspace, cyber threats, international law

* Emilia Chronowska, PhD Student, Kazimierz Wielki University in Bydgoszcz, e-mail: emilia.chronowska@ukw.edu.pl, ORCID: 0000-0001-6996-5503.

Introduction

Progressive technological development and cyberspace being an unlimited dimension of human activity create threats that are constantly evolving. In the context of the considerations undertaken, the key terms are: security, cyber threats, and cyberspace. The term cyberspace is used to describe the global domain of the information environment, which consists of interdependent networks formed by the information technology infrastructure, as well as any data contained in this domain including the Internet, telecommunications networks, and computer systems including processors and controllers[1]. Cyber threats are any threats that arise from the use of modes of electronic communications, primarily the Internet. Security is most often equated with a state of being free from danger. Given the above, cybersecurity is defined as the absence of threats in the Internet space, the absence of risks associated with the possibility of losing informational data.

Protecting cyberspace from the threats within it, as well as minimizing their negative consequences, is a very common security issue. States, but also international organizations and other non-state actors, are aware that secure cyberspace is a necessary condition for the stability of the functioning and development of the global information society. Increased awareness of the important role of cybersecurity is a consequence of new threats developing in cyberspace. This creates a need to develop and implement legal as well as organizational changes that would enable an appropriate level of cybersecurity[2]. The article aims to identify the main threats occurring in cyberspace, as well as to present the importance of security in this area for the proper development of the information society. The article also suggests directions for legislative and organizational changes that can improve cybersecurity.

The essence of cyberspace

The value of security in cyberspace is becoming an increasingly important issue due to the great importance of the aforementioned space to modern society as well as the state. Boguslaw Pacek and Romuald Hoffman define

1 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 9, p. 227.

2 T.R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, ibidem 2016, no. 15, p. 27–28.

cybersecurity as a state in which there is no risk of losing informational data in cyberspace. This unquestionably leads to the conclusion that the protected good is information[3]. The aforementioned authors treat cybersecurity issues as part of information warfare. This would indicate the legitimacy of considering information security as an inseparable part of national security. Consistent with this approach, it is important to emphasize that information security has numerous determinants, including: 1) information is a strategic resource of the state; 2) information, as well as the resulting knowledge and information technologies, is a fundamental factor of production; 3) information and communication technologies are an important factor of economic growth, and thus the information sector generates a significant part of national income; 4) information technologies are an extremely important element in the functioning of state security, including the armed forces; 5) information processing and transmission systems are important for decision-making processes in many sectors of the economy and social life; 6) mass media can be successfully used as tools for effective information disruption[4].

Information security can be defined very broadly. In the most general terms, it refers to a condition in which internal and external conditions enable a state to have, maintain, and develop an information society. The conditions that must be met to achieve such a condition are as follows: 1) there is no threat to the strategic resources of the state; 2) the decisions taken by the authorities are based on reliable, credible, relevant, accurate, and current information; 3) there are no disruptions in the flow of information between state authorities; 4) there are no disruptions in the operation of information and communications technology networks that form the state's critical information and communications technology infrastructure 5) the state can effectively guarantee the protection of classified information and personal data of citizens; 6) the right of citizens to privacy is not violated by state institutions; 7) public information is available to citizens, as well as to non-governmental organizations and representatives of the mass media[5].

In view of the above considerations, it can be said that cyberspace is a security environment, which involves the need for ongoing response to the threats occurring in this area and the introduction of appropriate changes

3 B. Pacek, R. Hoffman, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, p. 85.
4 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014, p. 57–58.
5 E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, p. 103.

in pragmatics, as well as in the legal and organizational dimension of security systems. Cyberspace is undoubtedly a phenomenon that has both a positive and a negative dimension. The positive dimension refers to the area of cooperation in cyberspace, which means an increase in the possibility of comprehensively satisfying social needs. Discussing these needs, we should first of all look at the aspect of self-development, self-fulfillment in various areas of life, in such spheres as education (the possibility of using global knowledge resources), scientific research (increase in knowledge resources and support for research), communication (development of social communication networks on a global scale), economics (the emergence of knowledge-based economy, various forms of „e-business"), culture, security, and also in the ludic sphere (cyberspace has become an international arena for games, entertainment, sport).

In parallel to the positive side, cyberspace also has a negative dimension. It is visible through phenomena that are a source of threats to internal (national) security, as well as external (international) security. The concept of „information warfare", which has its origins in military science, is gaining popularity. Information in cyberspace is simultaneously a resource, an object of attack, and a weapon. Information warfare is thus seen as a conflict in which information plays a key role, while at the same time this conflict concerns the physical destruction of infrastructure used by the opposing side to conduct operations. Piotr Sienkiewicz and Halina Świeboda emphasize that there is no agreed uniform definition of information warfare, however, it is nowadays believed that „cyberwar", „infowar", „netwar" cyberterrorism, information warriors, defense in cyberspace, and information warfare are just neologisms meaning the same thing – an extremely broad concept of information age warfare[6]. Such a general explanation needs to be clarified, which is also suggested by the aforementioned researcher. Sienkiewicz presents information warfare as the totality of offensive and defensive actions that are necessary to maintain an information advantage over the opponent and to achieve the desired military (political) goals. Two main objectives define the essence of such actions: to destroy the adversary's information resources, as well as the information systems they use, and to ensure the security of one's own information resources and the information systems they use[7].

6 P. Sienkiewicz, H. Świeboda, *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [in:] *Bezpieczeństwo teleinformatyczne państwa*, eds. M. Madej, M. Terlikowski, Warszawa 2009, p. 80.

7 P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, Kraków 2004, p. 30.

Selected threats in cyberspace

Information warfare in cyberspace takes the form of „cyber conflict". In this type of activity, success or failure is determined by the activities carried out in computer networks. Such conflict can take place in the form of: 1) activism, i.e. information and propaganda activities of a non-destructive nature (e.g. on social networking sites, forums); 2) hacktivism, which is a combination of activism and activities aimed at causing disruptions in the operation of specific computer systems (e.g. blocking access to selected servers); 3) cyberterrorism, which takes the form of politically motivated attacks on information systems, computers, networks, the aim of which is to destroy the infrastructure, the effect of which would be to force the government/organization to undertake a specific action or omission[8].

Conducting information warfare in cyberspace involves specific tools that simultaneously create the most serious threats that exist in cyberspace. These risks include: 1) attacks using malicious software (worms, viruses, malware – malicious software), the essence of such attacks consists in spreading programs in a computer system in order to change its operation or occupy the processor memory, disk space or other resources, resulting in blocking access to data; 2) logic bombs, which by activating new functions of logical elements of a computer aim at destroying hardware and software; 3) Trojan horses, i.e. programs making it possible to take action in a computer system without the knowledge of the rightful user (among others, copying data, deleting files); 4) sampling, i.e. gaining access to a computer and analyzing its characteristics; 5) authentication, consisting in impersonating users having access rights to the system; 6) theft, i.e. seizure of data (resources) present in the system by an unauthorized person; 7) modification or destruction of data; 8) unauthorized copying of files; 9) deletion of an attack target; 10) bypassing system security processes; 11) malicious components, which are chips that contain programs designed to allow unauthorized users access to the system and/or create design flaws; 12) transmission interception, i.e. gaining access to content sent between computers; 13) *DDoS* is the blocking of access to a website as a result of actions involving the transmission of a large packet of data from various sources to its address – this ultimately leads to the suspension of the server;

8 R.F. Ciriello, A. Richter, G. Schwabe, *Digital Innovation*, „Business & Information Systems Engineering" 2018, vol. 60, no. 6, p. 565–569.

14) *email bombing* is the action of sending huge amounts of data to the mailbox of an attacked user; 15) eavesdropping, i.e. tracking network traffic.

An increasing threat is posed by advanced persistent threat (ATP) attacks, which combine various types of tools, including but not limited to software and social engineering. Attacks of this type require a long period of preparation and are usually carried out by organized groups. The operations also involve a great deal of money and time to infiltrate the chosen target and launch the attack, resulting in data theft or damage or destruction of the computer system. A well-known example of an ATP-type attack was the Windows-based Stuxnet worm, which had the effect of delaying Iran's nuclear program, among other things[9].

Cybersecurity in light of European and Polish regulations

Due to the intense technological development, there is a clear need for regulating legal issues related to cyber security. The first difficulties occur at the stage of attempting to create normative definitions of acts and activities that pose threats in cyberspace. Under international law, such an attempt was made by the Council of Europe with the adoption of the Convention on Cybercrime in Budapest in 2001. The Budapest Convention defines individual key terms such as: information system, information data, service provider, and traffic data. In addition, the said Convention requires the Member States to criminalize many acts committed in cyberspace, which are categorized as follows: 1) crimes against the distrust, integrity, and availability of computer data and systems (illegal access, illegal interception of data, violation of data integrity, violation of system integrity); 2) computer crimes (forgery and computer fraud); 3) crimes by the nature of the information contained (unlawful and intentional production, offering, sharing, acquisition and possession of child pornography using an information system); 4) copyright infringement using an information system.

European Union law defines acts against cybersecurity in a very similar way. Directive 2013/40/EU obliges the Member States to take steps to punish as criminal offenses acts such as unlawful access to information systems, unlawful

9 A. Kohnke, D. Shoemaker, K. Sigler, *The Complete Guide to Cybersecurity Risks and Controls*, New York 2016, pp. 24–25.

interference with systems, unlawful interference with data, and unlawful interception of computer data transmissions[10]. Article 7 concerns tools for committing cybercrimes and includes the punishable acts of intentional development, sale, delivery for use, transporting, distributing, or otherwise sharing any of the tools: a computer program (designed or suitably adapted to commit any of the crimes outlined), a computer password, an access code, and other data that create the ability to access part or all of an information system. From the perspective of the Republic of Poland, the content of this Directive is very important since it is a binding legislative act.

The Polish Penal Code also contains regulations relating to acts against security in cyberspace. The legislature treats such threats in terms of information warfare. This issue is addressed in Chapter XXXIII – Crimes against Protection of Information. Acts that are considered crimes by the Polish legislator are regulated by articles 267, 268, 268a, 269, 269a, 269b[11].

Polish solutions in the area of cybersecurity are fully consistent with European regulations. The initiative „i2010 – A European Information Society for growth and employment" indicates that each Member State should develop its own action plan to ensure security in this area. The European Security Strategy and the Internal Security Strategy identify common areas, among which is cybersecurity. The shape that the Polish cybersecurity system has taken has also been influenced by the European Union's Cybersecurity Strategy: an open, secure, and protected space. It is also worth mentioning that European Union legal regulations link the concept of cybersecurity with the concept of information critical infrastructure included in the framework of the European Programme for Critical Infrastructure Protection. As a party to international conventions, Poland is important to the development of cybersecurity. The most important international documents in this area are mainly the Council of Europe Convention on Combating Terrorism from January 27, 1977, the Council of Europe Convention on Cybercrime from November 23, 2001, the Council of Europe Convention on the Prevention of Terrorism adopted in May 2005, and the Stockholm Programme with its Action Plan. The basic national documents that regulate cybersecurity are the Crisis Management Law, the Telecommunications Law, the Law on Informatization of Entities Performing Public Tasks, the Law on Provision of Electronic Services, and the Banking Law.

10 J. Barcik, T. Srogosz, *Prawo międzynarodowe publiczne*, Warszawa 2007, p. 135.
11 A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001, p. 150–153.

The strategic documents governing the Republic of Poland's cybersecurity are: Republic of Poland's Cybersecurity Strategy 2019–2024, Republic of Poland's Cybersecurity Policy, and Republic of Poland's Cybersecurity Doctrine[12].

No doubt evolving threats to cybersecurity create the need for introducing new cybersecurity solutions. The issue of security in cyberspace, as defined by the Polish Criminal Code, goes beyond the traditional framework of acts understood as criminal. In some, undoubtedly extreme, cases, it may take a form that, according to the text of the Constitution, will provide the basis for one of the states of emergency. On September 27, 2011, the President of the Republic of Poland, Bronisław Komorowski, signed an amendment to the Martial Law Act. The prepared draft amendment included the introduction of the concept of cyberspace into Polish law. It can be concluded that such an action was intended to provide an impetus for change and further legislative work in this area. Progressing computerization forces the necessity to develop and implement effective preventive, organizational, legal, and technical solutions that will enable the effective protection of citizens. The care and responsibility for cybersecurity efforts cannot remain solely the responsibility of the government, and should also be shared among the public, private sector, and NGOs. This would undoubtedly create the need for a common cybersecurity policy for entities within the public and private sectors. It also seems appropriate to establish an effective coordination system, the main objective of which would be to enable and improve the cooperation of the mentioned sectors, public and private, in ensuring the security of cyberspace. It is also very important to take actions aimed at raising public awareness of cyber threats and the possibilities of counteracting them and minimizing their negative effects. It seems reasonable to develop and implement educational programs in this area[13].

The bottom line is that there is no doubt that cyberspace has become a security environment. Continuous technological advances and developments are generating more numerous, complex, and evolving forms of threats that exist in cyberspace. This creates the need for changes (pragmatic, legislative, organizational) in the functioning of security systems. Creating an effective legal system that responds to the state's opportunities and challenges in cyberspace, as well as the threats in cyberspace, is an extremely difficult

12 M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, no. 22, p. 128–129.
13 Ibidem, p. 130.

task. This is because technological change is proceeding at an incredible pace. The nature of the environment and its highly interactive nature is also not insignificant. The apparent trend in international law towards viewing the individual as an equal actor in international relations is of great importance in relation to the information society – the network society.

National regulations, laws governing international cooperation, and security policies and strategies must be adapted to the changing cyberspace environment. One should emphasize the need for rapid response, but also for efficient response to the activities of small, mobile groups, which creates a new quality in the area of formulating legal regulations relating to state security in cyberspace. Networking in its technological dimension, but also in its social dimension with all its consequences, seems to be currently one of the most relevant concepts of the new security paradigm, both at the national and international level. It should also be acknowledged that ensuring cybersecurity is one of the most important political as well as research & development challenges.

Bibliography

Adamski A., *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu Konwencji Rady Europy*, Toruń 2001.

Aleksandrowicz T.R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, no. 15.

Barcik J., Srogosz T., *Prawo międzynarodowe publiczne*, Warszawa 2007.

Ciriello R.F., Richter A., Schwabe G., *Digital Innovation*, „Business & Information Systems Engineering" 2018, vol. 60, no. 6.

Grzelak M., Liedel K., *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" 2012, no. 22.

Kohnke A., Shoemaker D., Sigler K., *The Complete Guide to Cybersecurity Risks and Controls*, New York 2016.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014.

Nowak E., Nowak M., *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011.

Pacek B., Hoffman R., *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013.

Sienkiewicz P., Świeboda H., *Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej* [in:] *Bezpieczeństwo teleinformatyczne państwa*, eds. M. Madej, M. Terlikowski, Warszawa 2009.

Sienkiewicz P., *Wizje i modele wojny informacyjnej*, Kraków 2004.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 9.

Wybrane zagrożenia bezpieczeństwa w cyberprzestrzeni

Streszczenie

Autorka artykułu przedstawia wybrane zagrożenia bezpieczeństwa w cyberprzestrzeni, identyfikuje je oraz wskazuje ich ewolucyjny charakter. Cyberprzestrzeń stanowi sferę bez określonych granic geograficznych i politycznych, o wysoce interaktywnej naturze. Treść artykułu pokazuje istotną rolę bezpieczeństwa cyberprzestrzeni w kontekście budowy społeczeństwa informacyjnego, a także prezentuje najważniejsze uregulowania prawne zarówno międzynarodowe, jak i krajowe wraz ze wskazaniem propozycji kierunków zmian na poziomie krajowym, które pomogłyby zwiększyć bezpieczeństwo cyberprzestrzeni. Autorka podkreśla znaczenie regulacji legislacyjno-organizacyjnych w podejmowaniu problematyki.

Słowa kluczowe: bezpieczeństwo, zagrożenia, cyberprzestrzeń, cyberzagrożenia, prawo międzynarodowe