Cyberspace and Cybersecurity

Tomasz Zdzikot

Abstract The purpose of this chapter is to discuss two basic concepts—cyberspace and cybersecurity. The author describes the genesis of both and attempts to define them. In the introduction, the author briefly addresses the issue of the progress of information technology in recent decades and the impact of this factor on security. Then, he indicates the source of the term "cyberspace" and presents the definitions in American documents, doctrine and Polish law. Defining the concept of "cybersecurity", the author starts from the definition of the term "security". Then he presents selected definitions of this term. He also emphasizes that cybersecurity should be viewed broadly and that a definition should be made taking into account both the attacks by hackers or foreign forces and the "plain" failures.

1 Introduction

In April 1998, during a widely commented lecture on information security in an increasingly digital world delivered at the Georgia Institute of Technology in Atlanta, CIA Director George J. Tenet warned: "We are staking our future on a resource that we have not yet learned to protect".[1] As the reality changed, the people responsible for the security of states and citizens accurately anticipated the threats they would soon face on an unprecedented scale. The increasing digitization and automation of every area of life would make more and more processes without digital support impossible with each day. An increasing part of human activity is also moving to the web, and access to information and keeping constantly "in touch" have become, in many spheres, the basic determinants of individual and organizational success. At the same time, the ease of access to information, as well as to the

[1] Tenet (1998).

T. Zdzikot (✉)
Warsaw Bar Association, Warsaw, Poland
e-mail: tomasz@zdzikot.pl

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_2

technologies enabling its generation and dissemination, contributes to a constant increase in data supply.

In the past, a few centuries ago, the best university libraries had hundreds of volumes in their book collections. Thus, reading them all did not exceed the capabilities of a single reader. Today, hundreds of thousands of new books are published every year. In Poland alone, more than 36 thousand titles[2] were published in 2017, while the number of books published annually in other countries often exceeds 100 thousand. The global network aggregating knowledge, information and access to entertainment and communication platforms is also growing rapidly. It is estimated that every second the network grows by 30 GB of data, that is, as much as the entire Internet[3] covered 25 years ago, while the number of websites increased from just over 17 million to one billion from 2002 to 2014.[4] Every second, Internet users carry out hundreds of thousands of operations on various social networking, entertainment and transactional sites. According to data quoted by Edward Lucas, the number of Internet users has exceeded 3 billion, and in "richer countries almost all are Internet users – in the USA, 88% of Americans are online (...) In 2015, the number of e-mails sent exceeded 200 billion per day. This means that more e-mails are sent in two days than traditional letters for a year." According to J. Surma: "The daily average number of searches using the Google browser is around 3.5 billion. Assuming that each search is made by a different person, almost every second person on the planet makes one search a day! The number of Facebook users is 25% of the world's population. In the case of Poland, almost 70% of the population use Google and almost 60% are Facebook users".[5] Therefore, today we receive as much information every day as our grandparents did throughout their lives. At the same time, the concept of the Internet of Things (IoT), in which the devices of everyday use around us become part of a trans-boundary information exchange system, is developing extremely intensively. It is assumed that within a few years there will already be more than 50 billion devices permanently connected to the Internet in the world.

At the same time, it must not be forgotten that the digital world today cannot be regarded as an anchor of stability and security. It is also a space where organized crime groups actively and creatively use new tools, improving new methods of committing known crimes and creating completely new categories of crimes. At the same time, in geopolitical and institutional terms, it is an attractive place for many

[2] *BN: in 2017, the number of books published in Poland increased by 6%, http://www.pap.pl/aktualnosci/news,1436634,bn-w-2017-roku-liczba-wydanych-w-polsce-ksiazek-wzrosla-o-6-proc.html* Accessed on 7 July 2020.

[3] *Co może zdarzyć się w sekundę w Internecie? (2015). https://www.focus.pl/artykul/co-moze-zdarzyc-sie-w-sekunde-w-internecie* Accessed on 7 July 2020.

[4] *Ile waży praca? (2017) https://www.forbes.pl/technologie/jak-wiele-danych-produkujemy-kazdego-dnia/4mn4w69* Accessed on 7 July 2020.

[5] Surma (2017), p. 74; the author also states that: "Such a widespread use of Google, Facebook and other similar companies in the global economy is of great importance for the security of individual states and the whole world".

countries to pursue their political objectives, intelligence tasks or a manifestation of power. Actions in cyberspace can also be a preparation for military operations or an element of those already under way.

In view of the outlined changes in civilization and new challenges, the performance of the basic tasks of a state, which include ensuring internal and external security, requires an adequate response from the state administration today. It is necessary to adapt to a situation in which a new field of action is cyberspace, and the ability to ensure the digital security of citizens and to secure one's own networks and systems represent the fundamental elements of national security.

In the face of globalization, security in cyberspace has become one of the priority tasks in the internal affairs of each country, while at the same time affecting international security. Any serious disruption to the operation of cyberspace will affect citizens' sense of security, the security of business trading, the efficiency of public sector institutions and, consequently, security in general. Therefore, it has become necessary to implement legal solutions which will make it possible to organize an effective and efficient system for protecting the information resources of public entities, entrepreneurs and also citizens.

2 Definitions of Cyberspace

One of the areas which has been partially governed by law, and which can be distinguished in the legal system and in the duties of public administration, is cybersecurity, which is the subject of this monograph. Any consideration of this subject must be preceded by defining the meaning of the terms cyberspace and cybersecurity, taking into account the typology of possible threats.

Cyberspace is one of the many concepts discussed in this monograph, which must be considered to be highly underdefined, eluding a uniform approach. No uniform definition has yet been established at the national or international level that could be considered universally accepted, although numerous attempts have been made and are being made on the basis of legislation, programming, legal commentary and strategic and political documents, as well as in legal commentaries and literature (including popular literature). Even the etymology of the word cyberspace is ambiguous. According to the literature "it can only be said in general terms that it is a blend (hybrid) of two words – *kubernḗtēs*, which in Greek means a helmsman, a governor, to control, and the English word *space*".[6]

The term cyberspace was first used by the American science-fiction author William Gibson in his short story "Burning Chrome" published in the "Omni" magazine in July 1982. Cyberspace was also mentioned in his novel "Neuromancer", published 2 years later, as

[6] Banasiński (2018), p. 23.

> a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts (…). A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data.[7]

It is noteworthy that 37 years ago, several characteristic features of the digital reality that surrounds us today were captured in this way—its global nature, the aggregation of data from a huge number of sources, dispersed network architecture, graphical visualization of complex source codes, light as an information carrier.

According to the Dictionary of the Polish Language, "cybeprzestrzeń" (cyberspace) is "a virtual space in which communication between computers connected to the Internet takes place".[8] However, this approach focuses only on one of the dimensions of cyberspace. Many experts divide cyberspace into layers, distinguishing between the physical network (hardware—connections and computers), the logical network (software – network and service software, such as websites), and a kind of human network (people functioning in cyberspace).[9] Such a comprehensive approach may also serve to create a definition, such as that of Z. Trejnis and P. Trejnis, according to which "Cyberspace encompasses all information and communication means in a collection of networks, techniques, users and digital space, which in turn is assigned three layers: material, logical and informational".[10]

The US Department of Defense, while unifying military terminology, has also introduced a definition of cyberspace 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.[11]

Compared with the aforementioned division of cyberspace into three layers, it can be noted that this US military definition seems to ignore the human aspect—participants and users of cyberspace—and to focus solely on the infrastructural and logical aspects.

Interestingly, a uniform definition of cyberspace was not adopted by the North Atlantic Treaty Organization until 2019. According to the NATO Glossary of Terms and Definitions, cyberspace is "The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and

[7] Gibson (2009), p. 59; New York: Berkley Publishing Group, 1989; after: https://techterms.com/definition/cyberspace, accessed on 3.10.2020.

[8] https://sjp.pwn.pl/szukaj/cyberprzestrze%C5%84.html Accessed on 3.10.2020.

[9] For example, Crowther Alexander (2018), pp. 83–84 https://www.heritage.org/sites/default/files/2017-09/2018_IndexOfUSMilitaryStrength_CROWTHER.pdf Accessed on 3.10.2020.

[10] Trejnis and Trejnis (2017), p. 27 http://bobolanum.pl/images/studia-bobolanum/2017/03/StBob_2017_3_Trejnis.pdf Accessed on 3.10.2020.

[11] Department of Defence Dictionary of Military and Associated Terms (2010) (Joint Publication 1-02), p. 58 https://fas.org/irp/doddir/dod/jp1_02.pdf Accessed on 10.10.2020.

their data, including those which are separated or independent, which process, store or transmit data."[12]

In Poland, threats associated with cyberspace have already been mentioned in the "National Security Strategy of the Republic of Poland" of 2007, but without precise terminological specification.[13]

The first official definition of cyberspace was contained in the assumptions for the "Government Cyberspace Protection Programme of the Republic of Poland for the years 2009-2011", for the purpose of which it is understood as "a communication space created by a system of Internet connections".[14] An attempt was also made to distinguish the category of state and, specifically, Polish cyberspace by stating that

> State cyberspace is understood to be the communication space created by the system of all Internet connections within the state. In the case of Poland, state cyberspace is also referred to as the cyberspace of the Republic of Poland. The cyberspace of the Republic of Poland comprises, among others, information and communication systems, networks and services of particular importance to the internal security of the state, the banking system, as well as systems ensuring the functioning in the country of transport, communications, energy, water and gas infrastructure and healthcare information systems, the destruction or damage of which may pose a threat to human life or health, the national heritage and the environment on a significant scale or cause serious material losses.[15]

In the "Government Cyberspace Protection Programme of the Republic of Poland for the years 2011-2016" prepared by the Ministry of the Interior and Administration in June 2010, the definition of cyberspace was developed. The document states that it is "digital space for the processing and exchange of information created by information and communication systems and networks, including the links between them and relations with the users".[16] The cyberspace of the Republic of Poland, on the other hand, was closely linked to the territory by indicating that it is "cyberspace within the territory of the Republic of Poland and in locations outside the territory

[12] NATO Glossary of Terms and Definitions AAP-06 Edition 2018 https://nso.nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF Accessed on 3.10.2020.

[13] As part of the outlined challenges and threats to security, it was pointed out that one of them "may be the impact in cyberspace, directed at the information and communication systems and networks of critical infrastructure. Such actions may result in both material losses and the paralysis of important spheres of public life." *National Security Strategy of the Republic of Poland* p. 10. However, one of the objectives of economic security was to continue the development of "a modern, integrated electronic communication structure that would be resistant to failures and potential cybercrime attacks. This will require proper interaction between relevant ministries and agencies as well as private actors", p. 19, http://www.bbn.gov.pl/dokumenty/SBN_RP.pdf, Accessed on 3.10.2020.

[14] https://www.msz.gov.pl/resource/93e1e4c7-e129-41c7-8365-39dbad8b1c54:JCR, p. 4, accessed on 3.10.2020.

[15] Ibidem.

[16] Government Cyberspace Protection Programme of the Republic of Poland for the years 2011–2016.

where representatives of the Republic of Poland operate (diplomatic posts, military contingents)”.[17]

The Act of 30 August 2011 amending the Act on Martial Law and the Powers of the Commander-in-Chief of the Armed Forces and the Rules for Their Subordination to the Constitutional Authorities of the Republic of Poland and certain other Acts[18] had a significant impact on the establishment of the concept of cyberspace in the Polish legal system. As stated in the justification of the Presidential bill, the basic aim of the regulation was

> to take into account threats resulting from activities and events in cyberspace as a circumstance complying with the normative content of the reasons for the introduction of one of the states of emergency referred to in Articles 229, 230 and 232 of the Constitution of the Republic of Poland.[19]

The legal definition established for the purposes of the amendment, setting out cyberspace as

> space for the processing and exchange of information created by information and communication systems, as defined in Article 3(3) of the Act of 17 February 2005 on the Computerization of the Operations of Entities Performing Public Tasks including the links between them and relations with the users,

by virtue of the amending act in question, was added to the provisions of:

1. the Act of 29 August 2002 on Martial Law and the Powers of the Commander-in-Chief of the Armed Forces and the Rules for Their Subordination to the Constitutional Authorities of the Republic of Poland—where actions in cyberspace were also included as one of the reasons for the introduction of martial law by the President of the Republic of Poland, at the request of the Council of Ministers, on part or all of the territory of the country;
2. the Act of 21 June 2002 on the State of Emergency—actions in cyberspace that pose a threat to the constitutional system of the state, security of citizens or public order may constitute a basis for the Council of Ministers to adopt a resolution to submit a request to the President of the Republic of Poland to introduce a state of emergency;
3. the Act of 18 April 2002 on Natural Disasters—indicating at the same time that a natural disaster or technical failure may also be caused by events in cyberspace.

[17] Government Cyberspace Protection Programme . . . ., p. 6

[18] Act of 30 August 2011 amending the Act on Martial Law and the Competences of the Commander-in-Chief of the Armed Forces and the Rules for Their Subordination to the Constitutional Authorities of the Republic of Poland and certain other Acts, Polish Journal of Laws of 2011, No. 222, item 1323.

[19] Parliamentary paper No. 4355. http://orka.sejm.gov.pl/Druki6ka.nsf/0/0C7D2B7644A7B3C5C12578BD00339405/$file/4355.pdf, accessed on 3.10.2020.

The definition developed for the purpose of introducing to the aforementioned acts on emergency states, referring directly to their content,[20] was transferred to the "Government Cyberspace Protection Policy of the Republic of Poland", prepared in June 2013 by the Ministry of Administration and Digitization and the Internal Security Agency. The definition of the cyberspace of the Republic of Poland is basically a repetition of the one established on the basis of the discussed "Government Cyberspace Protection Programme of the Republic of Poland for the years 2011-2016."

An extensive definition of cyberspace is included in the "Cybersecurity Doctrine of the Republic of Poland" of 2015, according to which it is

> a space for the processing and exchange of information created by information and communication systems (groups of cooperating IT equipment and software that ensure the processing, storage, as well as sending and receiving of data through telecommunications networks by means of telecommunications terminal equipment appropriate for a given type of network and intended to be connected directly or indirectly to network terminations), including the links between them and relations with the users.[21]

Despite the lack of a single common definition of cyberspace, a number of common features have been identified:

1. a seamless, flexible and non-material nature;
2. lack of clearly and unambiguously identifiable boundaries;
3. decentralization;
4. lack of a centre of control and supervision over it as a whole;
5. universal accessibility;
6. digital information processing and calculations in real time with high accuracy;
7. numerical, hypertext, interactive and virtual nature.[22]

A number of common features of cyberspace are also noticed by the Supreme Audit Office, which, in its information on the results of the audit on the "Implementation of tasks in the field of protection of the cyberspace of the Republic of Poland

[20] The full definition is as follows:

> space for the processing and exchange of information created by information and communication systems, as defined in Article 3(3) of the Act of 17th February 2005 on computerisation of the activities of entities performing public tasks (consolidated text Polish Journal of Laws of 2020, item 346, as amended), including the links between them and relations with the users; pursuant to Article 2(1b) of the Act of 29th of August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Armed Forces and the rules for their subordination to the constitutional authorities of the Republic of Poland (consolidated text Polish Journal of Laws of 2017, item 1932, as amended), Article 2 (1a) of the Act of 21st of June 2002 on the state of emergency (consolidated text Polish Journal of Laws of 2019, item 1928, as amended) and Article 3(1)(4) of the Act of 18th April 2002 on the state of natural disaster (consolidated text Polish Journal of Laws of 2017, item 1897, as amended).

[21] Cybersecurity Doctrine of the Republic of Poland (2015) https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, accessed on 3.10.2020.

[22] Kasprzyk et al. (2015), p. 529.

by state entities", also attempted to formulate a specific definition, perceiving cyberspace as "a virtual area created inside and within the range of influence of IT and telecommunications equipment",[23] whose common features include global reach, easy access, efficiency, universality and relative "cheapness".

In its electronic glossary related to information society, the European Commission has proposed a definition of cyberspace that emphasizes the hardware and software layers, but excludes the user sphere. In this sense, cyberspace is the "virtual space in which the electronic data of worldwide PCs circulate".[24]

On the basis of legal commentaries and literature, an interesting definition of cyberspace has been provided by M. Lakomy, who, summing up his multi-faceted considerations on the understanding of the concept, finally concludes that, in practice, cyberspace is

> a domain for the processing, storage and transmission of information in digital form, based on the transmission of digital signals and electromagnetic radiation. It is an immaterial space in its essence, but one that functions through the ICT infrastructure that produces and transmits these signals.[25]

The author stresses that this domain is created by "every bit of data stored, processed and transmitted in computers and computer networks, and all other elements that make up the ICT infrastructure in the broad sense".[26] Importantly, M. Lakomy also emphasizes that computers and other devices that are not currently connected to the global network should not be overlooked in this context, because even though they are not connected, these devices

> can perform important functions from the perspective of the interests of individuals, businesses or entire societies and countries: they control machines, help with calculations, support education and development, and therefore have a significant impact on the functioning of various areas of human life.[27]

In addition, isolation from cyberspace can be temporary, impermanent and illusory, and computers can communicate with other devices even when they remain offline, for example using various types of physical data carriers.

C. Banasiński very rightly connects the individual layers (spheres) of cyberspace, noting that it consists of both tooling and the social component. Of course, this author also states that "The basic factor that makes up cyberspace is the material information and communication system, which is a set of cooperating ICT equipment and software ensuring the processing, storage, as well as sending and receiving of data by telecommunications networks by means of telecommunications terminal equipment appropriate for a given type of network.[28] C. Banasiński notes, however,

[23] https://www.nik.gov.pl/kontrole/P/14/043/, accessed on 3.10.2020.

[24] After Wasilewski (2013), p. 229.

[25] Lakomy (2015), p. 83.

[26] Lakomy (2015), p. 83.

[27] Lakomy (2015), p. 83.

[28] Banasiński (2018), p. 25.

that the focus on the infrastructural and logical sphere (which he collectively calls the instrumental sphere) leads to the omission or marginalization of the

> social component of cyberspace, which refers to cyber users, and which treats cyberspace as a complex environment resulting from the immaterial interaction between people, software and services on the Internet provided through technical devices and networks connected to it; an equally important, integral and interconnected element with the technical infrastructure is its relationship with people and the interaction between people related to its use.[29]

Other authors also draw attention to the need for a comprehensive approach to cyberspace, not only as an infrastructure domain. According to R. Tadeusiewicz, cyberspace is

> a set of hardware and software tools related to the techniques of collecting, processing, transmitting and sharing information, used by people to acquire knowledge and to communicate with other people. The most important, but not the only, component of cyberspace today is the Internet.[30]

Similar conclusions are also drawn by J. Rzucidło and J. Węgrzyn, who stated that the notion of cyberspace "certainly includes at least a specific type of infrastructure and processes that take place in it, or includes people and the relationships that exist between them through this infrastructure, as well as between them and this infrastructure".[31]

Legal commentators also draw attention to the legal difficulties, both international and national, associated with the nature and essence of cyberspace as a cross-border, immaterial creation, with an unlimited number of users.[32]

3 Definitions of Cybersecurity

In the theory of security studies, it is assumed that the concept of security (from the Latin *sine cura*—"without concern") is interpreted primarily as a state of peace, safety and no threat.[33] At the same time, however, "security" should also be understood as a process, thus emphasizing that security and its organization are constantly changing, and therefore cannot be considered to be permanently established and organized.[34] In this sense, security means "the continuous activity of individuals, local communities, states or international organizations in creating

[29] Banasiński (2018), p. 26.

[30] Tadeusiewicz (2010), p. 32.

[31] Rzucidło and Węgrzyn (2015), p. 144.

[32] Wrona (2015), p. 872.

[33] Ściborek et al. (2015), p. 26.

[34] Marczak (2011), p. 15.

the desired state of security".[35] Cybersecurity can also be defined both by reference to the desired state and as a continuous process leading to it.

Closer to the first interpretation is the legal definition introduced by the Act of 5 July 2018 on the National Cybersecurity System,[36] which gives priority to the term "resilience". According to Article 2(4) of this Act, cybersecurity is therefore "the ability of information systems to resist any action that compromises the confidentiality, integrity, availability and authenticity of processed data or the related services offered by those systems". This term is based on the definition of "security of network and information systems" in Directive 2016/1148,[37] taking into account the evolution of certain concepts (e.g. information system).

The strategic document adopted by the Council of Ministers in 2017, entitled the National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022, associates cybersecurity with the security of network and information systems and ICT security, using them interchangeably and treating them as synonyms. However, the interpretation set out in the document is consistent with the definition mentioned above, introduced into the legal framework by the provisions of the Act on the National Cybersecurity System, and focusses on the ability of

> information and communication systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

The definition established at the Community level in the Digital Single Market Glossary leads to an emphasis on action and processes aimed at ensuring cybersecurity. According to it, cybersecurity

> commonly refers to the safeguards and actions available to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein. The term cybersecurity also covers prevention and law enforcement measures to fight cybercrime.[38]

[35] Marczak (2011), p. 15.

[36] Act of 5 July 2018 on the National Cybersecurity System (Polish Journal of Laws of 2020, item 1369, as amended, hereinafter "NCSA").

[37] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU 2016 L 194/1) For the purposes of the provisions of the Directive, "security of network and information systems" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.

[38] Digital Single market Glossary, https://ec.europa.eu/digital-single-market/glossary, accessed on 3.10.2020;

According to C. Banasiński, cybersecurity can be reduced to “an undisturbed way of collecting, processing and exchanging information recorded and processed digitally”.[39]

The explicit process-oriented understanding of cybersecurity indicates that it is not about an existing or desired state, but “a process which consists of actions taken by technical and non-technical means to protect cyberspace, including hardware, software and information or data”.[40] This dynamic approach to cybersecurity (specifically the cybersecurity of the Republic of Poland) was also adopted in the already mentioned Cybersecurity Doctrine of the Republic of Poland, stating that it is

> a process of ensuring the safe functioning in cyberspace of the state as a whole, its structures, natural persons and legal entities, including entrepreneurs and other entities without a legal personality, as well as the information and communication systems and information resources at their disposal in global cyberspace.[41]

The community-created definition in the Cybrary glossary is also process-oriented, according to which cybersecurity are “the processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked”.[42] At the same time, the definition also stresses that cybersecurity requires broad knowledge of the possible threats, such as viruses or other malicious objects, and that identity management, risk management and incident management are the crux of cybersecurity strategies of an organization.

A comprehensive understanding of the term cybersecurity is proposed in the dictionary of the US Department of Homeland Security, according to which it should be defined strictly as the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. An extended definition is also available, referring to strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence,

[39] Banasiński (2018), p. 33.

[40] Wasiuta et al. (2018), p. 223.

[41] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf Interestingly, the document distinguishes between the cybersecurity of the Republic of Poland and the security of the cyberspace of the Republic of Poland as “a part of state cybersecurity comprising a set of organisational and legal, technical, physical and educational projects aimed at ensuring the undisturbed functioning of the cyberspace of the Republic of Poland with the public and private critical information and communication infrastructure that constitutes its component and the security of information resources processed therein.” Accessed on 3.10.2020.

[42] Full quote:

> Cyber Security are the processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires extensive knowledge of the possible threats such as Virus or such other malicious objects. Identity management, risk management and incident management form the crux of cyber security strategies of an organization.

https://www.cybrary.it/glossary/c-the-glossary/cyber-security/ accessed on 3.10.2020.

international engagement, incident response, resilience, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[43]

Among the numerous typologies, the one proposed by M. Lakomy, who, from the point of view of national security, has divided threats into structured and unstructured ones, is particularly noteworthy. The former are characterized by a high degree of organization of their sources, technical sophistication and, from the point of view of the attacker, domination of political, military, religious and economic motivations, and these include cyberterrorism, cyber espionage and military operations in cyberspace. Unstructured threats, on the other hand, are characterized by a low level of organization, generally posing a lesser threat to national security, with the dominance of political, social and individual motivations. According to the author, they include hacking, hacktivism, "patriotic hacktivism", and cybercrime in the strict sense.[44]

The threats to cybersecurity can also be divided by:

- subject: criminals, terrorists, state entities,
- motivation: the intention to obtain profit, to exert political pressure, to obtain information, to gain military advantage, a form of a joke, the desire to become known in a particular environment, to gain popularity or publicity,
- *modus operandi*: immediate or long-term action, action with publicity or concealed action".[45]

In my opinion, it is appropriate to define cybersecurity also through the prism of threats that hinder the achievement of the desired state and are a challenge to ongoing processes.

It can be assumed that, in the broad sense, cybersecurity will be threatened by failures, accidents and, finally, attacks. Of course, failures and accidents will most often be strictly dependent on technical conditions, or, for example, an unintentional human error or, in general, random events. This is not the case for attacks which are deliberate in nature.

References

Banasiński C (2018) Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni. In: Banasiński C (ed) Cyberbezpieczeństwo. Zarys wykładu, Warsaw

Crowther AG (2018) National Defense and the Cyber Domain, pp. 83–84 https://www.heritage.org/sites/default/files/2017-09/2018_IndexOfUSMilitaryStrength_CROWTHER.pdf. Accessed 3 Oct 2020

[43] https://niccs.us-cert.gov/about-niccs/glossary#C accessed on 3.10.2020.

[44] Lakomy (2015), p. 137.

[45] Wasiuta et al. (2018), p. 223.

Gibson W (2009) Neuromancer. Katowice

Kasprzyk R, Maj M, Tarapata Z (2015) Przestępstwa w cyberprzestrzeni. Aspekty technologiczne i prawne. In: Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne, Warsaw

Lakomy M (2015) Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice

Marczak J (2011) Bezpieczeństwo narodowe. In: Jakubczak R, Marczak J (eds) Bezpieczeństwo narodowe Polski w XXI wieku, Warsaw

Rzucidło R, Węgrzyn J (2015) Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni. Przegląd Prawa Konstytucyjnego 5(27)

Ściborek Z, Wiśniewski B, Kuc R, Dawidczyk A (2015) Bezpieczeństwo wewnętrzne. Podręcznik akademicki, Toruń

Surma J (2017) Cyfryzacja życia w erze Big Data. Warsaw

Tadeusiewicz R (2010) Zagrożenia w cyberprzestrzeni. Nauka 4

Tenet GJ (1998) Information Security Risks, Opportunities, and the Bottom Line. https://www.cia.gov/news-information/speeches-testimony/1998/dci_speech_040698.html. Accessed 3 Oct 2020

Trejnis Z, Trejnis PZ (2017) Polityka ochrony cyberprzestrzeni w państwie współczesnym. Studia Bobolanum 28(3)

Wasilewski J (2013) Zarys definicyjny cyberprzestrzeni. Przegląd Bezpieczeństwa Wewnętrznego 9

Wasiuta O, Klepka R, Kopeć R (2018) Vademecum bezpieczeństwa. Kraków

Wrona J (2015) Jurysdykcja państw a zwalczanie cyberprzestępczości. In: Pływaczewski EW, Filipkowski W, Rau Z (eds) Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy prawno-kryminologiczne, Warsaw

Tomasz Zdzikot attorney-at-law, a graduate of the Law Faculty at the Cardinal Stefan Wyszyński University in Warsaw. He also completed, among others, postgraduate cybersecurity studies at the Polish Naval Academy in Gdynia, the *Top Public Executive* program co-organized by IESE Business School in Barcelona and the Lech Kaczyński National School of Public Administration in Warsaw and the *Higher Defence Course* at the National Defence University in Warsaw. Former Deputy Minister of National Defence and Plenipotentiary of the Ministry of Defence for the security of cyberspace (2018–2020), creator of the program for developing the capabilities of the Polish Armed Forces to operate in cyberspace—"Cyber.mil.pl". Deputy Minister of Interior and Administration (2015–2018) and Government Plenipotentiary for the Preparation of State Administration Bodies for Cooperation with the Schengen Information System and the Visa Information System (2017–2018) Currently—CEO of the Polish Post. Author of numerous publications on cybersecurity issues as well as media law and new technologies. ORCID: 0000-0003-4369-7146.