

Review article

Security threats in cyberspace

Marian Kopczewski^{1*} , Zbigniew Ciekanski² , Julia Nowicka³ ,
Katarzyna Bakalarczyk-Burakowska⁴ 

¹ Faculty of Security Studies,
General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland,
e-mail: marian.kopczewski@awl.edu.pl

² Faculty of Economic and Technical Sciences,
Pope John Paul II State School of Higher Education in Biata Podlaska, Poland,
e-mail: zbigniew@ciekanowski.pl

³ Military Faculty, Institute of Information Operations, War Studies University, Warsaw, Poland,
e-mail: j.nowicka@akademia.mil.pl

⁴ Institute of Law, Administration and Security, Warsaw Management University, Poland,
e-mail: bury.alle@wp.pl

INFORMATION

Article history:

Submitted: 19 October 2021

Accepted: 29 August 2022

Published: 15 September 2022

ABSTRACT

The article is an attempt to highlight the main types of security threats in cyberspace. As literature provides a multitude of different approaches, standards, methodologies, and proposals for the classification of threats, the article focuses on threats to privacy and national ICT security.

Cyberspace is subject to increasingly sophisticated and targeted threats, while our growing reliance on cyberspace exposes our privacy to risks, giving rise to new and significant security gaps. Due to its specific characteristics, it generates serious threats to individuals as well as to national and international security. Depending on the research perspective we adopt, these threats are variable, multidimensional, and multifaceted in nature. Therefore, they require systematic analysis and response.

KEYWORDS

security, cyberspace, cybersecurity, cybercrime, cyber espionage

* Corresponding author



© 2022 by Author(s). This is an open access article under the Creative Commons Attribution International License (CC BY). <http://creativecommons.org/licenses/by/4.0/>

Introduction

The topics outlined cover concepts such as “cyberspace” and “cybersecurity” that are complex and have not been fully explored; therefore, it is impossible to analyse them in a comprehensive and exhaustive manner. The aim of the article is to merely signal selected issues related to security threats facing individuals, societies, and states in the domain of cyberspace. It will discuss two intersecting groups of threats: threats to privacy in cyberspace and threats to national ICT security.

Literature highlights that, in the case of cybersecurity, the problem lies not in the shortage of classifications and descriptions of threats but in their overabundance. We can speak of the multiplicity of different approaches, standards, methodologies, and proposals [1, p. 36].

It is worth noting that there is no uniform approach to the nature of cyberspace. Some researchers regard it as a physical space, while others claim that it has nothing in common with the material world, as “touchlessness” is its main attribute. Cyberspace is described as the fourth domain (fourth space) or as a new dimension of the human existence. The multiplicity of concepts gives rise to specific consequences; namely, the absence of uniform regulations on cyberspace in international law.

Cyberspace is subject to increasingly sophisticated and targeted threats, while our growing reliance on cyberspace exposes our privacy to risks, giving rise to new and significant security gaps. Due to its specific characteristics, it generates serious threats to individuals as well as to national and international security. Depending on the research perspective we adopt, these threats are variable, multidimensional, and multifaceted in nature.

1. Nature and classification of cyber threats

Over the centuries, privacy has always been the target of various intrusions and threats. Traditional threats include [2, p. 112]:

- a) interference with private, family, or domestic life,
- b) violation of the psychological or physical integrity of an individual, individual freedom of opinion or morals,
- c) injury to dignity, honour, or reputation,
- d) showing someone in an unfavourable light,
- e) disclosure of intimate facts relating to a person’s private life,
- f) violation of the secrecy of correspondence or disclosure of information obtained from the person concerned under conditions of confidentiality,
- g) disturbance and harassment of another person,
- h) misappropriation of another person’s name, nickname, or achievement,
- i) circulation of another person’s image.

The above-mentioned threats are regarded as “standard” threats, however, it should be remembered that the first privacy laws were enacted at the time when the Internet, smartphones, social networks, drones, biometric identification, and the Internet of things (IoT) were unknown.

Privacy monitoring has always been there; it is a socially accepted phenomenon which existed already in small communities, where people watched their neighbours to exert moral pressure and enforce the norms of the community [3, p. 2]. Modern-day monitoring means not only that we are being watched but also that information about a growing number of aspects of our lives is collected, recorded, and stored.

Privacy threats in cyberspace have been the subject of numerous studies, which sometimes classify and assess them in different ways. M. Rojszczak has proposed a classification of threats taking into account new information processing technologies [4, p. 50]: cybercrimes, profiling, cyber-surveillance, disclosure of information, loss of control over information.

Without going into a deeper analysis of this classification, we need to emphasise that the first category, namely cybercrimes, is an extremely broad set and includes a wide range of

threats, in which privacy is only one of the targets. Threats from cybercrimes have been placed within a specific framework in the so-called Budapest Convention [5]. Cybercrimes have been classified into four essential groups: offences against confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences, and offences related to infringements of copyright and related rights [5, Art. 2-9]. Each of these groups refers to privacy threats in some degree, whether directly or indirectly.

The problem of threats in cyberspace has been analysed broadly by M. Lakomy. Although he did not relate them directly to people's privacy but to the national ICT security, many of the threats he identified certainly apply to people's private lives [6, p. 115-181].

Some authors have formulated a catalogue of threats related directly to privacy, which includes [7, p. 3-6]:

- a) Snooping (cyber snooping) – refers to i.a. advertisements offering software that enables activity on a computer to be monitored. In many cases, this type of software is not only insidious but also criminal,
- b) Harassment, stalking (cyber stalking) – cyber stalking involves various forms of stalking, such as following the posts of the persons concerned, recording their personal details, i.e. contact and address details, recording their likes, downloading their photos, lists of friends, etc.,
- c) Identity theft – the term phishing is widely used to describe an offence that involves digitally impersonating another person to gain a profit. It is often committed through the use of another person's login details or through unauthorised use of another person's digital/electronic signature to sign a contract online,
- d) Vishing – comes from the words voice and phishing. Vishing involves using a telephone to defraud a user. Simply speaking, it is a data scam performed in a voice conversation over the phone,
- e) Website defacement – it is intended to mislead people visiting a website, usually first-time visitors. It involves an attack on a website that alters its visual appearance. The perpetrators hack into a web server and replace the hosted website with their own website,
- f) Copyright infringement.

Published sources also contain studies referring to technologies that threaten privacy (privacy-destroying technologies). They can be divided into two categories: technologies facilitating the collection of so-called raw data and technologies that enable the processing, collation, and analysis of that data [8, p. 1468]. This distinction does not seem to be entirely accurate, as data processing and analysis are also enabled by new forms of data collection. Privacy-destroying technologies can also be classified on the basis of their social context. We can speak of technologies focusing on characteristics of individuals whose data is being collected (e.g. citizens, employees, patients, drivers, consumers). We can also distinguish between technologies on the basis of different types of observers (e.g. intelligence agencies, law enforcement, tax authorities, insurance companies, shopping mall security, e-commerce sites, concerned parents, etc.).

The Big Data market also poses threats to privacy. The term Big Data has been used to refer to a set of phenomena related to the production, consumption, collection, and analysis of large sets of data created by numerous different sources, in a great number of formats and in unprecedented volumes, which can be transferred at unprecedented speeds [9, p. 39].

Big Data has always been associated with vast scale and complexity. The proliferation of Internet networks and services gave rise to companies such as Yahoo, Google, Apple, Amazon, YouTube, Twitter, and Facebook. They extract value from large data sets for the purposes of service definition and improvement, trend analysis, product discovery, and all types of marketing and advertising. Big Data companies have developed special tools to transfer, process, store, and analyse data. The techniques used so far in classic data management systems have proved to be inadequate at best.

Collecting data in large databases allows for creating personal data profiles. When the data is available to others, they can create personal profiles for the purposes of targeted marketing, or, in rare cases, even for blackmail. For some people, just knowing that their actions are being recorded can have a chilling effect on their behaviour, openness, etc. Customers may consider the fact that the seller knows about their income, level of debt, or other personal data an unwarranted intrusion into their privacy [8, p. 1469-1470].

2. Internet of things and threats to privacy

Internet of things is a concept that assumes the ubiquitous presence of various things/objects in the environment, which are able to interact with one another and work together with other things/objects through wireless and wired connections, and unique addressing schemes, to create new applications/services, and to achieve common goals [10, p. 6121]. In this context, the challenges of creating a smart world are enormous. The situation where the digital and virtual realities combine to create smart environments makes energy, transport, cities, and many other areas much more intelligent. Yet, while it enables services that enhance the quality of everyday life, the Internet of things poses a huge threat to privacy at the same time [11, p. 2731].

In its 2015 document entitled Internet of Things Position Paper on Standardization for IoT Technologies, the European Commission recognised it as “A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network” [12, p. 13].

The evolving nature of the Internet of things in terms of technology and functions, as well as the emergence of new ways of interacting with it, result in specific threats to privacy and privacy-related challenges. According to some experts, they can essentially be divided into seven types: identification, localisation and tracking, profiling, privacy-violating interaction and presentation, lifecycle transitions, inventory attack, and linkage [11, p. 2734-2738]. We need to characterise them briefly.

Identification

It denotes the threat of permanent association of, for example, the name and surname, address, or any nickname, with a specific person and data relating to that person. Thus, the threat consists in associating an identity with a specific context of privacy violation. At the same time, it enables and amplifies other threats, such as profiling and tracking people, or combining different sources of data. The threat of identification is currently the most dominating threat. It can materialise through surveillance data technology, face databases (e.g. from Facebook), fingerprint devices, etc.

Localisation and tracking

It denotes a threat related to identifying and registering a person's location in time and space. Tracking requires some form of identification to link a location to a particular person. Currently, tracking is enabled by various means, such as the global positioning system (GPS), Internet traffic, or mobile phone localisation. This category includes i.a. stalking with GPS trackers, disclosure of private information, such as illness, and discomfort caused by the awareness of being watched.

Profiling

This threat has been signalled earlier. Profiling denotes the possibility of compiling information about individuals to determine their interests through correlation with other profiles and data. Profiling methods are used most frequently for personalisation in e-commerce (e.g. in recommendation systems, newsletters, and advertising), as well as for internal optimisation based on customer demographics and interests. Examples of situations in which profiling leads to violations of privacy include price discrimination, unsolicited advertising, social engineering, and faulty automated decisions.

Privacy-violating interaction and presentation

This threat concerns the transmission of private information through a public medium and its disclosure to outsiders in the process. Many IoT applications, such as smart retail, transport, and healthcare, require intensive interaction with the user. It is conceivable that in such systems information will be provided to users of smart things in their environment, for example, through advanced lighting installations, speakers, or video screens. And, conversely, users will be able to control systems in new, intuitive ways, using the things that surround them; for example, by moving, touching and speaking to smart things. Since many of these interaction and presentation mechanisms are public by their very nature, it implies that outsiders are able to observe them.

Lifecycle transitions

Privacy is at risk when smart things disclose personal data once they are no longer in use. Two changes to the IoT are likely to exacerbate problems related to the lifecycle of devices. Firstly, smart objects will interact with many people, other things, systems, and services and will collect the information in product history logs. Data collected by some applications can be highly sensitive; this is the case, for example, with health data collected by medical devices. However, even the collection of simple usage data (e.g. location, duration, and frequency of usage) can reveal a lot about people's lifestyles. Secondly, as replaceable everyday objects, such as light bulbs, become smart, the sheer number of such things entering and leaving people's private sphere will make it increasingly difficult to prevent data disclosure.

Inventory attack

Inventory attacks refer to the unauthorised collection of information about the existence and properties of personal items. Interconnectedness is one of the evolving features of IoT. As a consequence, smart things are becoming subject to a kind of online "interrogation" that can be performed from any location by legitimate entities (for example owners and authorised users of the system). Unauthorised parties may test this and use it to make an inventory of items located in a specific place, such as household, an office building, or a workplace.

Linkage

This threat consists in linking various, previously separated systems in such a way that linking data sources reveals (either true or false) information, which the subject did not disclose and did not intend to disclose to isolated sources. Users feel concerned about wrong inferences being made on the basis of combined data from various sources, which may be collected in different contexts and incorrectly compiled.

An example of privacy breach by linking data sources and systems is an increased risk of re-identification of anonymised data. Working with anonymised data is the standard approach to privacy protection, however, combining different sets of anonymised data may enable re-identification.

3. Cyber security (ICT security) threats

The discussion should begin with threats described in normative documents. The European Directive on attacks against information systems and replacing Council Framework Decision 2005/222/EU distinguishes four main types of threats [13, Art. 3-6]:

- a) Illegal access to information systems – intentional and unlawful access to the whole or any part of an information system when committed in breach of security measures, at least in cases which are not minor,
- b) Illegal system interference – intentional and unlawful hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, at least in cases which are not minor,
- c) Illegal data interference – intentional and unlawful deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, at least in cases which are not minor,
- d) Illegal interception – intentional and unlawful intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data, at least in cases which are not minor.

At the same time, it listed specially designed computer programmes, computer passwords, access codes, and similar data enabling access to the whole or part of an information system, as tools used for the dissemination of the above-mentioned threats (offences) [13, Art. 7].

In 2015, the European Parliament released a study on cybersecurity, which relies on the definition proposed by the International Organisation on Standardisation and defines a threat as a potential event which, once it develops into an actual event, may cause an unwanted incident that may harm an organisation or a system [14, p. 25]. Taking the most popular analyses of cybersecurity threats into account, the European Parliament classifies threats according to the following criteria:

- a) Targets of threats (individual, organisational, supply chain, societal) [14, p. 28],
- b) Threat actors (individuals or groups that carry out or intend to carry out cyberattacks – states, profit-driven criminals, ideologically motivated hackers or extremists) [14, p. 29-30],
- c) Threat tools (malware, banking trojans, ransomware, botnets, exploits) [14, p. 33-37],
- d) Impact on information security (unauthorised access, destruction of information, modification of information, disclosure of information, denial of service DDoS).

It is worth pointing out that advanced persistent threats (APT) are regarded as extremely serious threats. The perpetrators of such attacks engage in systematic monitoring and theft of data, and in some cases may resort to destruction. The intention of the perpetrators is to remain anonymous and undetected. APT attacks are most often the domain of states that direct them against particularly sensitive areas such as technology, national security, and critical infrastructure.

Other attempts to structure cybersecurity threats are to be found in literature. One of them is the so-called hybrid (multidimensional) model for threat classification, which takes the following classification criteria into account [15, p. 492]:

- a) Security threat sources: internal or external,
- b) Security threat agents: human, environmental, and technological,
- c) Security threat motivation: malicious or non-malicious,
- d) Security threat intention: intentional or accidental,
- e) Threats impacts: destruction of information, corruption of information, theft/loss of information, disclosure of information, denial of use, elevation of privilege, and illegal usage.

As we mentioned before, M. Lakomy divided ICT security threats into unstructured and structured ones; moreover, he characterised cyber warfare. In the first group, he included: hacking, patriotic hacktivism, and cybercrime. In the second group, he described cyber terrorism, cyber espionage, and military operations in cyber space. However, he made a reservation that the character of this classification is purely conventional, as the cyberspace is a highly dynamic environment and threats often intersect and do not fit into a clear-cut description. Let us briefly characterise the main ones here.

Hacking

It is the oldest form of “exploiting computer security errors and gaps, which gives origin to virtually all challenges encountered today” [15, p. 138]. Hacking refers to activities that aim to break the security of digital devices such as computers, smartphones, tablets, or even entire networks. Although the aims of hacking are not always destructive, currently most references to hacking and hackers describe them as unlawful activities of cyber criminals, motivated by financial gain, protests, gathering information (spying), or even a kind of “entertainment”. Hacking computers amounts to modifying computer hardware and software to achieve a goal that extends beyond the original intent of their authors [16, p. 90].

Hacktivism

Hacktivism, an unstructured form of cybersecurity threats, is a type of hacking activity motivated by a higher purpose; namely, the promotion of certain values, attitudes, and ideas, which may be political, social, or economic [6, p. 142]. This activity involves hacking into a computer system and making changes in it to influence a person or an organisation.

Hacktivism use a wide range of techniques to achieve their goals, including doxing, denial of service (DoS) attacks, anonymous blogging, information leaks, and website replication. The aim of hacktivism is to circumvent government censorship to help citizens bypass national firewalls (or help protesters organise themselves), and to use social media platforms for the promotion of human rights [17].

4. Cybercrime

As mentioned above, an attempt to put this category into a legal framework was made in 2001 by the Council of Europe, which resulted in the adoption of the so-called Budapest Convention. The Convention did not define cybercrime; the meaning of the term needs to be determined on the basis of the offences described in the document.

The United Nations has adopted a narrow and broad definition of cyber-crime. The first definition applies to all actions of the nature of IT operations that are aimed at breaching an IT security system. The broader definition of cyber-crime covers “all acts committed using or concerning computer systems or networks” [18, p. 203].

The term “cybercrime” is not defined in Polish government documents regulating cybersecurity issues. It is also not defined in the National Cybersecurity System Act of 4 July 2018. In the “Cyberspace Protection Policy of the Republic of Poland” adopted in 2013, cybercrime was defined very briefly as “an offence committed in cyberspace” [19, p. 5].

The Penal Code does not penalise cybercrime as such; instead, it penalises acts which make up this concept, namely, strictly computer-related crimes [20, Art. 267-269]; offences related to the use of networks, ICT systems, and new technologies [20, Art. 286, Art. 278 § 2, Art. 285, Art. 287, Art. 276, 270 § 1]; offences committed with the use of computers and ICT networks [20, Art. 190 § 1-2]; computer-related offences against sexual freedom committed against a minor [20, Art. 202, Art. 200a § 1-2]; offences against honour [20, Art. 212, Art. 216].

Attempts to define cybercrime have also been made in Polish academic literature. The authors of the “Vademecum of ICT security” define it as “all illegal activities carried out by persons who use information technology and telecommunication networks in a way that violates legally protected goods” [18, p. 202]. According to K.J. Jakubski, it is “a criminological phenomenon covering all criminal behaviours related to the functioning of electronic data processing which directly harm the processed information, its carrier and circulation in the computer and in the whole system of computer connections, as well as the computer equipment itself and the right to a computer program” [21, p. 31]. Meanwhile, P. Sienkiewicz considers cybercrime to be “the use of cyberspace to commit common and organised criminal acts targeting the resources of individuals and/or organizations (institutions)” [22, p. 97].

5. Cyber terrorism

Some specialists describe cyber terrorism as the “new terrorism” of our time. The term was defined more precisely by Dorothy E. Denning to the House Committee on Armed Services in May 2000. She stated that “Cyber terrorism is a convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives” [23, p. 4].

Cyber terrorism is an attractive weapon to modern terrorists for a number of reasons. It is less expensive than traditional terrorist methods. All a terrorist needs is a personal computer and Internet connection. It remains more anonymous than traditional methods of terrorism. The range and number of targets for cyber terrorism are enormous, which guarantees that vulnerabilities can be found.

Cyber terrorism can be conducted remotely, which is especially attractive to terrorists. It requires less physical training, psychological investment, mortality risk, and travel than

conventional forms of terrorism. It can also have a direct impact on more people than traditional methods of terrorism can, thus generating more media publicity, which is what terrorists want the most [23, p. 6].

Cyber espionage

R. Nogacki and M. Ciecierski remarked that “espionage is systematically entering cyberspace and taking control of it” [24, p. 202]. It is the case because cyberspace has unique properties relevant to spies. First of all, it is more difficult to identify the perpetrators. They are able to steal information remotely, without revealing their identity, and sometimes even falsifying it. They act above borders, which makes it difficult to determine their location. Second, “theft of information in cyberspace can be perpetrated by an individual, a weak state, or a small enterprise, which is resourceful enough to hire a gifted hacker who is able to make use of malware or to steal sensitive information” [24, p. 204].

6. Military operations in cyberspace

Experts believe that we are currently dealing with the militarisation of the Internet, which is a source of tension in international relations. Superpowers and large countries have started to create separate armed forces responsible for combat in cyberspace. M. Lakomy pointed out that the establishment of the United States Cyber Command (USCYBERCOM) by the United States in 2009 has symbolic significance [6, p. 165]. Other countries, such as the UK, Russia, and China, have followed its example.

The defence and security strategies of many countries already provide for military responses to cyber attacks. The United States has reserved the right not so much to respond adequately, as to respond with all means, while the Polish martial law treats attacks from cyberspace as equal to an armed attack on the territory of the Republic of Poland [25, p. 21].

Literature usually treats military activity in cyberspace in two ways. Some authors see them as a manifestation of cyber warfare, while others regard it as information warfare. Referring to the reflections of F. Schreier, who believes that information warfare extends far beyond combat in cyberspace, M. Lakomy suggests that armed operations in cyberspace are a narrower category [6, p. 166]. He points out that this domain may be used to achieve specific military effects, which, however, do not have to be components of cyber warfare.

Conclusions

Literature provides us with a multitude of approaches to and classifications of threats in cyberspace. For example, one of the significant threats, namely cybercrime, is an ambiguous term, not covered by a rigid legal framework and classified differently by various experts; what is more, the dynamic technological development in computer sciences is not making the adoption of a fixed definition of it any easier.

Cyberspace is subject to increasingly sophisticated and targeted threats, while our growing reliance on cyberspace exposes our privacy to risks, giving rise to new and significant security gaps. In this rapidly expanding domain, threats come from individuals who may have various motivations, criminal and terrorist organisations, and even states.

There is a clash between fundamental values in cyberspace: state sovereignty and security clash with the human rights, especially the right to freedom; moreover, the security of the

state clashes with citizens' right to privacy. These conflicts require serious analysis but they certainly do not facilitate the combating of external threats. On the other hand, the measures taken by the native state to ensure security and to counteract these threats are restricted by legal mechanisms for privacy protection. The so-called information governance is a major threat to citizens' security in cyberspace [26, p. 228]. It should be understood as a legally justified possibility for the state and its bodies to interfere with the private lives of citizens.

Acknowledgement

No acknowledgement and potential founding was reported by the authors.

Conflict of interests

All authors declared no conflict of interests.


Author contributions


All authors contributed to the interpretation of results and writing of the paper. All authors read and approved the final manuscript.


Ethical statement

The research complies with all national and international ethical requirements.

ORCID

Marian Kopczewski  <https://orcid.org/0000-0003-0402-0477>

Zbigniew Ciekankowski  <https://orcid.org/0000-0002-0549-894X>

Julia Nowicka  <https://orcid.org/0000-0002-0778-0519>

Katarzyna Bakalarczyk-Burakowska  <https://orcid.org/0000-0002-2649-0779>

References

1. Lisiak-Felicka D, Szmit M. *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*. Kraków: European Association of Security; 2016.
2. Braciak J. *Prawo do prywatności*. Warszawa: Wydawnictwo Sejmowe; 2004.
3. Solove DJ. *Conceptualizing privacy*. California Law Review. 2002;90(4):1088-155.
4. Rojszczak M. *Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji* [dissertation]. Warszawa: Uniwersytet Warszawski; 2018.
5. Ustawa z dnia 12 września 2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r. (Dz. U., poz. 1514).
6. Lakomy M. *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego; 2015.
7. Kaur G. *Privacy Issues in Cyberspace: An Indian Perspective*, [online]. 14 August 2020. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3673665&download=yes [Accessed: 1 July 2021].
8. Froomkin AM. *The Death of Privacy?* Stanford Law Review. 2000;52(5):1461-543.
9. Mortazavi M, Salah K. *Privacy and Big Data*. In: Zeadally S, Badra M (eds.). *Privacy in a Digital, Networked World*. Cham: Springer; 2015, p. 37-55.
10. Patel KK, Patel SM. *Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges*. International Journal of Engineering Science and Computing. 2016;6(5):6122-31.

11. Ziegeldorf JH, Morchon OG, Wehrle K. *Privacy in the Internet of Things: threats and challenges*. Security and Communication Networks. 2014;7:2728-42.
12. *Internet of Things Position Paper on Standardization for IoT Technologies*. European Research Cluster on The Internet of Things. European Communities; January 2015.
13. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW (D. Urz. UE L 218/8 z 14.8.2013).
14. *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*. Study. PE 536.470. European Parliament. Directorate General for Internal Policies. Policy Department; 2015.
15. Joujnja M, Rabaja LBA, Aissab AB. *Classification of security threats in information systems*. Procedia Computer Science. 2014;32:489-96.
16. Pal Bera S. *Overview of Hacking*. IOSR Journal of Computer Engineering. 2016;18(4):90-2.
17. Frankenfield J. *Hackivism*, [online]. Portal Investopedia. 26 August 2021. Available at: <https://www.investopedia.com/terms/h/hackivism.asp> [Accessed: 20 September 2021].
18. *Vademecum bezpieczeństwa teleinformatycznego. Tom 1 (A-M)*. Wasiuta O, Klepka R (eds.). Kraków: Wydawnictwo LIBRON – Filip Lohner; 2019.
19. *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*. Warszawa: Ministerstwo Administracji i Cyfryzacji. Agencja Bezpieczeństwa Wewnętrznego; 2013.
20. Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny (Dz. U. z 1969 r. Nr 13, poz. 94).
21. Jakubski KJ. *Przestępczość komputerowa – podział i definicja*. Przegląd Kryminalistyki. 1997;(2).
22. Sienkiewicz P. *Ontologia cyberprzestrzeni*. Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki. 2015;9(13):89-102.
23. Weimann G. *Cyberterrorism How Real Is the Threat?*, [online]. Available at: <https://www.usip.org/sites/default/files/sr119.pdf> [Accessed: 30 September 2021].
24. Ciecierski M, Nogacki R. *Bezpieczeństwo współczesnej firmy. Wywiad, szpiegostwo, ochrona tajemnic*. Warszawa: Wydawnictwo Studio EMKA; 2016.
25. Aleksandrowicz TR. *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*. Przegląd Bezpieczeństwa Wewnętrznego. 2016;15(8):11-28.
26. Pryciak M. *Prawo do prywatności*. Studia Erasmiana Wratislaviensia. 2010(4):211-229.

Biographical note

Marian Kopczewski – prof. DSc Eng., full professor, researcher at the faculty of Security Studies, Military University of Land Forces in Wrocław. A graduate of several universities, previously worked at polytechnic and other universities. At the university, he lectures, popularising modern teaching techniques and manages the diploma process in the field of security, crisis management and diploma seminars. In his scientific work, he focuses on analyzing and assessing the possibilities of using information systems in management and teaching, as well as national and internal security systems, including European and Euro-Atlantic political and military integration processes. He is the author and co-author of about 1000 various domestic and foreign publications, including several monographic publications thematically related to national security and IT systems. Participant and active speaker at many conferences and scientific meetings. He manages scientific and research works on a domestic and foreign scale, as part of this work he has promoted 9 doctors and is a promoter to several more. He is a member of the Polish Society for Production Management, the Polish Society for Security Sciences, and the Polish Association of Creative Teachers. His hobbies include: reading, active holidays in the mountains, and swimming.

Zbigniew Ciekankowski – PhD Eng., associate professor at the Warsaw Management University and Pope John Paul II State School of Higher Education in Biała Podlaska. Visiting professor

at the Brest State Technical University in Brest. His academic interests focus on issues related to crisis management and broadly understood security, considered especially from the military perspective. He is an expert on management in hierarchical institutions and the author of dozens of books and more than two hundred papers in security sciences, management, and quality, published at home and abroad.

Julia Nowicka – PhD, assistant professor at the Institute of Information Operations at the War Studies University and associate professor at the Institute of Law, Administration and Security at the Warsaw Management University. She is a sociologist specialising in social psychology. She holds a PhD degree in social sciences in the discipline of Defence with specialisation: Management of Public Institutions. Her interests and academic output combine the following disciplines: security sciences, social communication and media studies, management and quality studies. The researcher's interests focus on aspects of communication in the field of security. She provides expert consultancy in the area of media exposure and communication crises in the public administration and private sectors. Author of numerous research publications in the field of security studies, management and quality, and communications, published at home and abroad.

Katarzyna Bakalarczyk-Burakowska – Master in Pedagogy, expert at the Department of Classified Information Protection and Control at the Police Training Centre in Legionowo, Inspector for Personal Data Protection, author of numerous publications on cybersecurity and data protection. Participant of numerous academic conferences and international conferences on cybersecurity, cyber terrorism, and personal data protection in cyberspace.

Zagrożenia bezpieczeństwa w cyberprzestrzeni

STRESZCZENIE

W artykule podjęto próbę naświetlenia głównych kategorii zagrożeń bezpieczeństwa w cyberprzestrzeni. Z uwagi na fakt, iż w literaturze istnieje mnogość różnych ujęć, standardów, metodyk i propozycji klasyfikacji zagrożeń, skoncentrowano się na zagrożeniach prywatności oraz bezpieczeństwa teleinformatycznego państwa.

Cyberprzestrzeń podlega w coraz większym stopniu wyrafinowanym i ukierunkowanym zagrożeniom; rosnące uzależnienie od cyberprzestrzeni naraża naszą prywatność, stwarza nowe i znaczące luki w zabezpieczeniach. Z uwagi na swoje specyficzne właściwości generuje w jednakowym stopniu poważne zagrożenia dla jednostki, bezpieczeństwa narodowego i międzynarodowego. Zagrożenia te, w zależności od przyjętej perspektywy badawczej, mają charakter zmienny, wielowymiarowy i wielopłaszczyznowy. Wymagają systematycznej analizy i reakcji.

SŁOWA KLUCZOWE

bezpieczeństwo, cyberprzestrzeń, cyberbezpieczeństwo, cyberprzestępczość, cyberspiegostwo

How to cite this paper

Kopczewski M, Ciekanski Z, Nowicka J, Bakalarczyk-Burakowska K. *Security threats in cyberspace*. Scientific Journal of the Military University of Land Forces. 2022;54;3(205):415-26. DOI: 10.5604/01.3001.0016.0040.



This work is licensed under the Creative Commons Attribution International License (CC BY).

<http://creativecommons.org/licenses/by/4.0/>