Akademia Sztuki Wojennej

Cybersecurity and Law

Nr 1 (9) 2023

Warszawa 2023

ISSN 2658-1493

Adres redakcji:
Akademia Sztuki Wojennej w Warszawie
Akademickie Centrum Polityki Cyberbezpieczeństwa
Al. gen. A. Chruściela „Montera" 103
00-910 Warszawa
e-mail: cyber.law@akademia.mil.pl

Skład, druk i oprawa: Wydawnictwo Akademii Sztuki Wojennej, zam. nr 1027/22, nakład 100 egz.

Spis treści

Katarzyna Chałubińska-Jentkiewicz*

Freedom of speech in international regulations in the face of digital media development

Abstract

In the face of technological development, the relationship between freedom, including freedom of speech, and security – especially its digital variety, namely cybersecurity – is a particularly difficult relation.

It should be pointed out that the international plane is an indispensable dimension of human rights protection, since it is in the international plane that new standards in the field of human rights are created, which are then brought into the system of domestic law and the practice of states. Meanwhile, the existence of international legal regulations increasingly often becomes a guarantee of the effectiveness of domestic legal systems. International institutions often become the institution of appeal for individuals and a lever to force state governments to respect fundamental human rights and freedoms. Support for individuals, communities or nations fighting for their rights, and their success in this struggle, contribute to the formation of a new democratic international order.

Key words: freedom of speech, cybersecurity, digital media, regulation, international law

* Assoc. Prof. Katarzyna Chałubińska-Jentkiewicz, PhD, War Studies University in Warsaw, Head of the Academic Centre for Cybersecurity Policy, e-mail: kasiachalubinska@gmail.com, ORCID: 0000-0003-0188-5704.

Introduction

The contemporary process of penetration of the idea of natural rights of the individual into positive law being a formal legal expression of human rights highlights the special importance of eighteenth-century declarations, especially the „United States Declaration of Independence" of 4 July 1776 and the French „Declaration of the Rights of Man and of the Citizen" of 26 August 1789. This latter declaration, like the former, provides in Art. 1 that „Men are born and remain free and equal in rights", while Art. 2 emphasises that „the aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, and Safety"[1].

To systematise and diagnose the instruments used today to protect the freedom of speech, it is first necessary to characterise the conditions of limitations, noting that this refers to limitations on the exercise of freedoms and not to limitations on the freedom itself. According to constitutional provisions, there are four categories of limitations: limitations that are necessary in a democratic state for the protection of its 1) security; 2) public order; 3) protection of the natural environment; 4) health and public morals; 5) freedoms and rights of other persons. In this respect, it is particularly important to address the issue of limitations of the freedom of speech on the grounds of security. The question of what nature of security is involved needs to be resolved. In particular, when it comes to digital media, the key question is whether we are dealing with broadly defined cybersecurity, or whether it is about specific cybersecurity of the state. The article attempts to present the conditions that change the concept of the protection of freedom of speech as a basic rule governing the digital world.

International regulations vs. human rights and freedoms

The idea of natural human rights and their protection has gradually pervaded emerging international law. On the progressive process of the internalisation of law Izabela Malinowska writes „entailed the need to regulate human rights by international law. A number of universal, regional and dedicated treaties have been adopted"[2], making up the international law on human rights and

1 K. Motyka, *Prawa człowieka. Wprowadzenie. Wybór źródeł*, Lublin 2004, p. 34–35, 116–118, 119–121.

2 I. Malinowska, *Prawa człowieka i ich międzynarodowa ochrona*, Warszawa 2004, p. 5.

their protection. Many such treaties were concluded between World War I and World War II[3], but international law on human rights law noticeably developed after World War II[4]. This development was, on the one hand, the result of the traumatic experience of the war and, on the other hand, the expression of desires and aspirations of the entire international community to ensure that people will not have to go through such experiences in the future, to build a lasting foundation for freedom, justice and peace in the world – conditions that are necessary for a sustainable, comprehensive security system, closely connected with respect for human dignity and rights.

Among the endeavours undertaken in the sphere of the international protection of human rights and freedoms, the most effective are international protection systems, which consist of comprehensive instruments such as the legal basis, i.e., a document-convention that constitutes binding international law, an institution or a set of institutions to ensure compliance with the document by the states parties, and a set of methods, mechanisms and procedures that make it possible to monitor compliance by the states with the assumed obligations, and in the case of violations, to influence the states to act under the agreement. These endeavours, linking the issue of security with the respect for fundamental human rights and freedoms, are reflected, *inter alia*, in the United Nations' universal system for the protection of human rights and freedoms.

The first essential document was the „United Nations Charter". Article 1.2 states that its purpose is: „To achieve international cooperation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and fundamental freedoms for all without distinction as to race, sex, language, or religion"[5]. It also includes provisions outlining tasks for all nations and states in respecting fundamental human rights and freedoms. Furthermore, it provides institutional foundations for the development of an international system for the protection of human rights. Further elements of this system are formed by „The Universal Declaration of Human Rights, the Covenants on Human Rights", as well as other conventions and declarations that explicitly highlight the problem of human dignity[6].

3 K. Motyka, op. cit., p. 38.

4 Ibidem, p. 125; *Prawa człowieka. Dokumenty międzynarodowe*, elaborated and translated by B. Gronowska, T. Jasudowicz, C. Mik, Toruń 1993.

5 *United Nations Charter* [in:] ibidem, p. 14.

6 Cf. A. Łopatka, *Deklaracja godności człowieka*, „Res Humana" 1999, no. 1, p. 3–8.

In the introduction to *the* „Universal Declaration of Human Rights" adopted on 10 December 1948, it is stated that „[...] recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world. Concluding that [...] the disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind and resulted in the advent of a world in which human beings shall enjoy the freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people".

Subsequent UN documents dated 1966 having a character of international agreements, which include the „International Covenant on Civil and Political Rights" with the „First Optional Protocol" and the „International Covenant on Economic, Social and Cultural Rights", created an elaborate system for the protection of the rights of individuals. They represent the first ever international acts containing a rich catalogue of human rights and freedoms, obliging the states that ratified them to implement them. They, therefore, serve a similar function to constitutions in individual states.

UN bodies responsible for protecting human rights include the Human Rights Council, the Treaty Committees, the United Nations High Commissioner for Human Rights (UNHCHR) and the International Criminal Court.

To respect the rights stipulated in these and other documents[7], the Economic and Social Council set up Committees. States Parties are required to submit periodic reports on the implementation of the provisions contained in these legal acts.

In the European system of protection of the individual, the „European Convention for the Protection of Human Rights and Fundamental Freedoms", adopted in 1950, played a special role. Referring unquestionably to „the

7 Documents that make up the UN system: the United Nations Charter, the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Optional Protocol to the International Covenant on Civil and Political Rights, the Second Optional Protocol to the International Covenant on Civil and Political Rights aimed at the Abolition of the Death Penalty, the International Covenant on Economic, Social and Cultural Rights, the International Convention on the Elimination of All Forms of Racial Discrimination, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, the Convention on the Rights of the Child, the Convention on the Elimination of All Forms of Discrimination against Women, Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women, the Convention relating to the Status of Refugees, Standard Minimum Rules for the Treatment of Prisoners, the Declaration of Philadelphia, and the United Nations Millennium Declaration.

Universal Declaration of Human Rights", it formulated its catalogue of guaranteed rights, the content and scope of which continue to be developed by subsequent optional protocols and bodies for the protection of those rights operating under established procedures[8].

The primary body upholding the rights guaranteed by the „Convention for the Protection of Human Rights and Fundamental Freedoms" and the protocols thereto is the European Court of Human Rights, based in Strasbourg. When considering complaints, the Court examines the grounds for the limitations applied by the state, including legal regulations that could be dictated by security reasons. First, whether the interference was provided for by domestic law. According to the Court's interpretation, the law should be understandable to the citizen and precise enough for the citizen to anticipate the consequences of a certain behaviour, and whether it is consistent with the rule of law. Second, whether the purpose of the interference was legitimate, e.g., protecting morals, security, and the rights of other persons. Third, whether the interference was „necessary" in a democratic society, or whether there was a strong social need for the limitation. Fourth, whether the interference was proportionate to the legitimate purpose.

Determinants of digital media development

The technological revolution, the first stage of which was the creation of the digital world, has entered another transformation process that clashes with issues that are crucial for democratic societies, as they relate directly to the foundations and axiology of freedom. The sense of uncertainty about tomorrow, stemming from the inability to assess and control the technological future, has recently taken real shape, as the new digital society is a community whose rules are unknown, and the new social order, without defining common values and

8 Other instruments for the protection of human rights developed in the system of the Council of Europe include: the European Social Charter (1961), the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (1987), the European Framework Convention for the Protection of National Minorities (1995), the European Convention on the Exercise of Children's Rights (1996), the Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (1997), the European Convention on Nationality (1997), the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and the European Charter of Local Self-Government.

establishing protective norms, raises a concern. Technological corporations are becoming the decision-makers in matters that were previously the domain of public authorities and courts. This also applies to such an important sphere as freedom of speech and the digital media that operate based on it.

This is particularly important in relation to social media, as online communities are a powerful force with tremendous power of communication and expansion, as well as the potential for manipulation, due to the specific nature of online technologies. The term social media refers to computer technology that facilitates the sharing of ideas, thoughts and information through virtual networks and communities. Social media is based on the Internet and provides users with the fast electronic communication of digital content such as personal data, documents, videos and photos. Users access social media via computers, tablets or smartphones using software, or web-based applications. In 2021, 3.96 billion social media users were reported worldwide. In one day, 4.2 billion photos were „liked" on Instagram. On top of that, nearly 100 million new photos/posts are created on IG every day. The use of the „Story" function has increased by 100 million posts since 2017. Facebook is the seventh most visited site in the world. 78% of users have used Facebook to find new products and services. Facebook is the most popular marketing platform for any social media channel. Nowadays, media policy is developed predominantly based on online coverage and is changing the thinking about the impact of media messages on the recipient – the online user. This is influenced by the peculiarities of digital media, which include: the ease of commenting – everyone has access to a computer and this can be done practically at any time; the belief in anonymity; the stoking of emotions – gossip portals often use clickbait (usually headlines that have nothing to do with the truth), as they make money from the number of displayed ads accompanying the message; the cult of beauty and perfection.

Modern social media are creating a new reality, often conveying it differently than the factual situation requires, presenting only selected facts, masking some information, falsifying the message and manipulating public opinion. Such situations are key to the development of the phenomenon of post-truth and disinformation. Facts are becoming less important in shaping public opinion than appealing to emotions and beliefs. In the post-truth era, core values are under threat due to cynicism and the extreme breakdown of all once cherished media attributes, e.g., truth, honesty and journalistic integrity. It is also a process of arguing with beliefs rather than facts. With the abundance of information and the publication of various articles that are reprints

of foreign-language publications, it is more and more difficult for publicists and readers to verify sources. However, liberty and freedom of expression carry great responsibility and the need to use them by acting with due diligence, in good faith and by following professional ethics. All the phenomena indicated hereinabove, observed in the digital media space, have an impact on public opinion and the public sphere.

Redefining freedom of speech

An attempt to redefine freedom of the press was made by Jürgen Habermas, who introduced a definition of „public sphere", recognising it as a domain of social life where public opinion can be formed. This public character applies both to the characteristics of the message itself and the audience, and to the functions of social media and their sphere of influence. Diversity, pluralism and the freedom of expressing an opinion and view allow for the analysis and selection of the best alternative. It is a privilege of the public sphere but also a duty of public authorities that at the times of digital transformation, relevant institutions using instruments legitimised by the will of societies be allowed to speak in defence of fundamental freedoms, including freedom of speech, against the decision-makers – the owners of online platforms, created as a result of the prevailing economy of digital messages. This is due to the obvious need to support the individual, the citizen, society as a whole, as well as individual social groups who, in the face of superseding the rules of the real world by the rules of the digital world, need to make their bones in both material and political areas, in their identity, in their language, as well as in their axiology and the democratic institutions that are close to them.

However, the principle of the freedom of social media still underpins the functioning of all digital players and determines the role of digital media in any society. The historical pedigree of this freedom dates back to the enactment of the Constitution of the United States of America, and after World War II the idea of the freedom of speech became a permanent component of the catalogue of rights and freedoms of the individual, a fundamental part of the standard of a democratic state. The inclusion of the idea in widely adopted international documents contributed to its dissemination, as well as the determination of its content. However, the attributes of freedom of speech are changing and the rule itself is not unlimited in the face of new threats that are emerging due

to the development of digital media and the expansion of audiences to previously unimaginable proportions.

One of the key provisions in the area of international regulations is Art. 19(1) of the International Covenant on Civil and Political Rights, which opened for signature in New York on 19 December 1966, (ratified by Poland on 3 March 1977, Journal of Laws of 1977, no. 38, item 167; hereinafter: „the Covenant"), which states that „Everyone shall have the right to hold opinions without interference". Paragraph 2 of this article provides that „everyone shall have the right to freedom of expression", while clarifying that this right shall include „freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or print, in the form of art, or through any other media of his choice".

In turn, Art. 10 of the European Convention on Human Rights, „Freedom of Expression", ensures that everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary for a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the authorities.

And in the sphere of EU law, Art. 11 of the EU Charter of Fundamental Rights (2010/C 83/02), „Freedom of expression and information", introduces the rule that everyone has the right to freedom of expression. This right shall include the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers, and the freedom and pluralism of the media shall be respected.

Like the documents indicated above, the Polish Constitution provides for the protection of civil rights and freedoms, including the freedom of speech (Art. 14 and 54 of the Polish Constitution). The Constitutional Court has repeatedly stressed that the provision of Art. 54 of the Polish Constitution encompasses three freedoms: the freedom to express opinions and to acquire and disseminate information.

The latter, i.e., the freedom to disseminate information, includes both making content available to entities individually chosen by the disseminator

and disseminating information, i.e., making it available to the public, meaning non-individualised addressees, especially through the mass media, that is social media. The principle of the freedom of speech and social media is a rule that encompasses both the privilege and the duty to disseminate information because a free press exercises the civic right to reliable and responsible information and it serves the entire society.

Limitations on the exercise of constitutional freedoms and rights may be imposed only by statute, and only when they are necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights. Thus, any limitations of this freedom must result from a legal norm and be justified by the indicated grounds enumerated in the constitution.

There is no doubt that international documents have guided the normative content of the idea of the freedom of speech in written constitutions; especially those that came into force during the period of an established catalogue of rights and freedoms in a democratic state. From the content of the provisions in international documents, it is clear that in the era of the digital revolution it is not only about the freedom of speech in the traditional sense, but a broadly defined freedom of expression, guaranteeing both the freedom of opinion and the freedom of form of expression, within the limits set by the legal norm and not by the principles of the self-regulation adopted by BIG tech.

It should be emphasised that the freedom of social media was considered a fundamental element of politics that allowed the balance between the governed and the ruled, and any unjustified, unregulated encroachment into this sphere by law violated the democratic principles of the rule of law. Today, however, digital democracy, which has resulted in the development of digital media, is also a kind of instrument for generating threats.

Freedom of expression is one of the foundations of a democratic society, a condition for its development and the self-realisation of individuals. This freedom must not be limited to information and views that are received favourably or perceived as harmless or indifferent. The role of journalists is to disseminate information and ideas concerning matters of public interest and public importance. This is in close connection with the right vested in the public to receive information. As indicated above, freedom of expression may be affected by limitations. However, there is no doubt that the most elementary condition for limiting this freedom is the requirement of statutory regulation. Consideration of the fundamental role of freedom of speech

in a democratic state under the rule of law dictates particularly strict scrutiny of the precision of the provisions of laws introducing limitations in the exercise of this freedom. It should be noted that the Committee of Ministers of the Council of Europe has determined that legislator's intervention is not the most appropriate means of reconciling media freedom with other rights and values. Modern media plays a special social role in the information and culture-making spheres. Opinion-forming and creative functions are also important as regards moral values and attitudes. In the face of information development, it is important to emphasise its importance as a „transmitter" of a certain system of values, dictated by public interest needs. Freedom of the press was considered „the palladium of all civil, political and religious rights" (Junius), „a necessary feature of the nature of a free state (Blackstone), „a conversation between the government and the people" (Hegel), „a thought provoker" (Voltaire). „Freedom of the press has allowed England to become a uniquely modern society that has blurred the traditional boundaries between stability and confusion, truth and falsehood, the real and the possible"[9]. The need to guarantee free media and freedom of speech stems from the media's role in the public sphere, where public discourse occurs and public opinion is formed.

However, it should be emphasised that freedom of communication is one of the consequences of civil and personal freedom in the broadest sense, encompassing all forms of communication between people, while the secrecy of correspondence is a much narrower concept, related primarily to the right of everyone to respect his or her private life, and to his or her right to keep secret the content of communications addressed to other persons or institutions. Such a concept of the right to correspondence is influenced primarily by the content of Art. 8 (1) of the European Convention on Human Rights, which links the right to respect for correspondence with the right to respect for private life, family life and the home. This right is indirectly connected with the right of secrecy of correspondence. The secrecy of correspondence is also violated when, as a result of the loss of someone else's correspondence, real conditions (danger) have been created that allow, with a high degree of probability, third parties to become acquainted with its contents. Such violation of the secrecy of correspondence may take place with respect to the correspondence of a person deprived of liberty. The court also stated that the secrecy of

9 Cf. J. Keane, *Media a demokracja*, London 1992, p. 26.

correspondence applies to all situations and places, including cyberspace. In the context of the aforementioned provisions of the Constitution and the European Convention on Human Rights, it should be assumed that this right can be limited by law. However, within the limits to which it was granted, no one may violate it, in particular by preventing correspondence from reaching the addressee[10].

However, despite changing the paradigm of the role and the importance of the freedom of speech, ethical principles pertaining to the profession of journalism are still crucial. The job of a journalist is to serve the public and the state. A journalist has a duty to act in accordance with professional ethics and principles of community life, within the limits prescribed by law. A journalist has the right to refuse to execute an official order if he or she is expected to publish something that violates the principles of integrity, objectivity and professional diligence. A journalist may refuse to publish press material if changes have been made to it that distort the sense and meaning of his or her version. These rules are still relevant in the digital world.

The right of access to the Internet

Modern states are not indifferent to many aspects of new media activity, due to their responsibility for all elements of economic and social life, at every stage of the development of a community, they significantly influence the regulation of the media market. In implementing their strategies, public authorities use certain instruments of law. The role of public authorities in the period of social transformation that is taking place as a consequence of the ongoing processes of social media digitisation is related, in particular, to regulation and regulatory functions. Social changes in the face of globalisation as well as national identity are categories external to the organisational principles of the development of a network society, adopted by a given state, contrasting its message with the cult of technology, the power of flow and the logic of markets. Sometimes,

10 Last year, a huge amount of Facebook data circulated publicly, splattering information from some 533 million Facebook users across the Internet. The data includes such things as profile names, Facebook ID numbers, email addresses and phone numbers. Data of more than 35 and a half million Facebook users from Italy leaked to the network, followed by the French (19.8 million), the British (11.5 million), the Spanish (more than 10 million) and the Germans (6 million). The persons affected include 2.5 million Internet users from Poland.

however, it is precisely such values that can be used in a way that contradicts democratic principles and basic human rights, and provide a compelling argument for limitations of the right to acquire information and make it available, which is a fundamental right and constitutional principle expressed in Art. 54 of the Polish Constitution. The crisis as regards the freedom of speech and access to information is a progressive phenomenon that can be observed especially in the states with an underdeveloped tradition of democratic values (such as Central Asian States, China, and the Russian Federation), where national limitations have a significant impact on fundamental values. Meanwhile, given the new conditions and technical possibilities, the legal system that guarantees the rationing of traditional, classic social media seems anachronistic in the face of digitisation, at least in some areas. One of the new prerequisites for exercising the freedom of speech is access to infrastructure. An important premise for recognising Internet access as a fundamental human right becomes apparent. These transformations are contributing to the creation of a new cultural policy, the basic premises of which may be the place of development of „the policy of informationalism". This space is often the new media, where values and problems derived from the life experiences of people living in the information age are relevant.

The crisis regarding freedom of speech and access to information[11] is a progressive phenomenon that can be observed especially in the states with an underdeveloped tradition of democratic values, where national limitations significantly impact on fundamental values. Meanwhile, in view of the new conditions and technical possibilities, the legal system that guarantees the rationing of traditional, classic social media seems anachronistic in the face of digitisation, at least in some areas. Public authorities face numerous difficulties in the process of limiting freedom of speech due to the specificity of an ICT network, and the multi-functionality of mobile devices that are increasingly cheaper and improved (Moore's Law). Digitisation, which has transformed the system of media operation, may also justify limitations of the right to communicate. Thus, it can be concluded that social development

11 Access to information can be restricted for securiry reasons. For security of information, see: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015; M. Karpiuk, K. Chałubińska-Jentkiewicz, *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015; M. Czuryk, *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015; K. Chałubińska-Jentkiewicz, M. Karpiuk, *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

is characterised by communication processes. The term „communication" comes from the Latin verb „communico", „communicare" (to make common, to connect, to give someone a message, to confer) and the noun „communio" (commonality, a sense of connection). The term „communicate something" also means „to make something known, to convey some information, to give notice of something"; while to „communicate" means „to keep in touch with someone, to come to an understanding". Thus, communication is a social process, which means that it refers to a specific relationship. Such a relationship, in the case of public communication, is of institutional, public, and group character, but also increasingly often, due to the development of message individualisation, is a process directed at the individual and his or her rights.

On the one hand, some countries and international organisations are considering recognising Internet access as a fundamental and universal human right while, on the other hand, many governments are considering tighter controls of content and the right to block technical means of transmitting digital content. According to a BBC World Service survey of 27,000 adults in 26 countries, nearly four out of five people worldwide believe that access to the Internet is a basic right. In this context, it is important to recall one of the most important principles reported at the World Summit on the Information Society (Geneva 2003 – Tunisia 2005). Participants at this conference declared „a common desire and commitment to building a common Information Society, where everyone can access, utilise and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights".

Net neutrality

Another important element of the regulation and rationing of the new media at the international level is net neutrality, which means the principle applicable to Internet access service, according to which Internet traffic of the same type is treated equally, i.e., without discrimination, restriction, slowdown or interference, regardless of the sender, receiver, content, device, service or application. End-users have the right to access and distribute information and content of their choice, to use and deliver applications and services of their choice, as well as to use terminal devices of their choice as part of Internet

access service. Blocking, slowing down or degrading traffic transmitted on the Internet is prohibited, unless it serves, in particular, the purpose of 1) enforcing a court decision; 2) ensuring the integrity and security of the network or services provided over the network, end-user devices, as long as equivalent types of traffic are treated equally; 3) preventing or minimising the effects of temporary and exceptional network congestion, as long as equivalent types of traffic are treated equally.

Poland's proposal on net neutrality, regarding the text of the draft regulation of the European Parliament and the Council, „Connected Continent", defines Internet access services by referring to the best effort model with explicit emphasis on the validity of the principle of net neutrality. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access, and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) no. 531/2012 on roaming on public mobile communications networks within the Union, introduced a definition of the term „Internet access service" which means a publicly available electronic communications service that provides access to the internet, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used. Article 3 of the Regulation introduces the right to access and distribute information and content via an ICT network. This also includes the right to use and provide applications and services, and to use terminal equipment of their choice, irrespective of an end-users or provider's location or the location, origin or destination of the information, content or application. It should be noted that not every state adopts a policy of open internet access. It should be emphasised here that, according to an estimate from the report Privatizing Censorship, Eroding Privacy, the number of states where arrests are made for online publications has increased by half since 2013. Since June 2015, the police in 38 states around the world have arrested citizens over their social media activity.

Open access to resources

An important element influencing network access policy and the accompanying rule of open access to resources is the issue of public mentality, the fear of losing control over data and information, and the issue of resource security.

The regulatory concept is based on three complementary pillars: adjustment of the regulatory framework, including the adoption of legal measures, soft law measures and policy measures, prioritisation of normative solutions including open data principles in research, development and innovation activities and infrastructure programs, coordination and the exchange of experience among member states with benchmarking. The objective of an open access policy is to provide access subject to the protection of intellectual property rights. The necessary research includes technical, organisational and legal aspects.

Redefining the objectives of international regulation in the area of media activities

In the wake of the evolution of new technologies, regulatory changes must take place. This process is parallel to technological development and the development of digital technology while increasing consumer needs and globalisation. The development of new technologies as well as the related processes of social change require a new regulatory approach, and also a redefinition of the public interest objectives and the duties of the state in the process of regulating those areas that hit key issues related to the functioning of the individual – the citizen, the market and the state. The processes of the convergence of previously differently conceived regulatory areas are contributing to a special kind of conflict in the area of arrangements for the scope and level of new regulations. When talking about the changes brought about by new technologies, we must remember that this phenomenon requires an interdisciplinary approach, combining the knowledge and viewpoints of specialists, and experts in the fields of economy, sociology, technology, media, political science, psychology and culture, and security sciences. Modern living conditions largely depend on the level of the information and communications technology that functions in a given state. We are currently witnessing radical changes in how societies and the global economy operate as a result of the expected spread of innovative ICT solutions. The ideological basis supporting this exchange is freedom of speech, and freedom of communication. Thanks to new social media techniques (information and communication networks, the Internet), completely unknown ways of the functioning of individuals in families and in professional and public life have appeared. With the development of digital technology and social changes, also associated with the process of the formation of so-called digital democracy, new areas of human

activity commonly referred to as the information and communication network environment, more broadly understood as cyberspace, have emerged. They affect all aspects of life. This applies to social relations, the economy, state-individual relations and the exercise of fundamental rights of the individual. Open and free cyberspace allows the exchange of cultures and experiences between states, communities and individuals, enabling interactions and the exchange of information, and, consequently, the exchange of knowledge, experience and technology. Therefore, it can be said that a lack of regulation ensures the exchange of technology and, consequently, the development of innovation. However, this is just a small piece of a very complex issue – the development of modern technologies and the risks associated with them.

In the present conditions of the functioning of an individual in cyberspace, it seems necessary to take new steps to establish international norms and, before that, to redefine the principles and values that are standard in the real world. Freedom in the online environment also requires security and protection.

The evaluation of digital markets based on freedom on the net reports clearly defines the relationship between public authorities and the digital media environment. Especially in the case of such a sensitive issue of regulating the content of electronic media, including media services provided on the net, for instance, in connection with disinformation. This thesis contradicts the principle of the democratic will of a sovereign state pursuing its public interest, especially concerning issues of a cultural nature, where the equally fundamental principles of subsidiarity and proportionality must be taken particularly seriously. The issue of the regulation of infrastructure and the use of instruments typical for preventive censorship of contents is significant mainly owing to the constant change in the position and roles of market users, in the global international sphere. Technological changes have contributed to the growing importance of infrastructure operators at the expense of content providers. And because of this phenomenon, the digital media world will be regulated using the level of technical access to the network. The examples of selected states support the thesis that regulation by public authorities in the network area, more or less offensive, is a way to strengthen the need for power, even in those so far most libertarian areas.

Cyber security as a rationale for international regulation

Social changes associated with the development of civilization stimulate democratic processes, and provide a space for the achievement of various economic goals, but can also be a place for undesirable activities. This applies to virtually every sphere of human life, including freedom of speech. The risk of threats to the individual is increasing in proportion to the process of weakening the state as a structure and institution, and this is particularly true of the information and communication network cyberspace based on it. As a result, individuals and citizens lose their sense of security. Ensuring cybersecurity[12] is one of the most important objectives of states' efforts in the international arena. The state, using its attributes of power, employs a variety of legal instruments and legal institutions designed to protect the public interest, public morality or national security. The situation of the weakening of the state and its institutions, as a consequence of digital change, threatens directly national security and, consequently, individual security like no other. For this reason, it becomes necessary to determine the status of the individual and the citizen in the face of the development of cyberspace. This also applies to values such as freedom of speech. If the protection guarantee is analysed, it becomes necessary to supplement its scope with a diagnosis of civic duties and limitations related to cybersecurity, according to the principle „homo persona moralis est quaternus spectatur tanquam subiectum certarum obligationum atque iurium certarum"[13].

Bibliography

Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2.

Chałubińska-Jentkiewicz K., Karpiuk M., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii. Wybrane zagadnienia*, Warszawa 2015.

12 For cybersecurity, see: K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Karpiuk, *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2; K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, no. 2; M. Karpiuk, *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

13 H. Conrad, *Individuum und Gemeinschaft in der Privatrechtsordnung des 18 und beginnenden 19 Jahrdundderts*, Karlsruhe 2006, p. 16.

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.
Conrad H., *Individuum und Gemeinschaft in der Privatrechtsordnung des 18 und beginnenden 19 Jahrdundderts*, Karlsruhe 2006.
Czuryk M., *Informacja w administracji publicznej. Zarys problematyki*, Warszawa 2015.
Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Position of the Local Government of Commune Level in the Space of Security and Public Order*, „Studia Iuridica Lublinensia" 2019, no. 2.
Karpiuk M., Chałubińska-Jentkiewicz K., *Prawo bezpieczeństwa informacyjnego*, Warszawa 2015.
Keane J., *Media a demokracja*, London 1992.
Łopatka A., *Deklaracja godności człowieka*, „Res Humana" 1999, no. 1.
Malinowska I., *Prawa człowieka i ich międzynarodowa ochrona*, Warszawa 2004.
Motyka K., *Prawa człowieka. Wprowadzenie. Wybór źródeł*, Lublin 2004.
Prawa człowieka. Dokumenty międzynarodowe, elaborated and translated by B. Gronowska, T. Jasudowicz, C. Mik, Toruń 1993.

Wolność słowa w regulacjach międzynarodowych w warunkach rozwoju mediów cyfrowych

Streszczenie

W warunkach rozwoju technologii szczególnie trudną relację stanowi związek wolności – w tym wolności słowa i bezpieczeństwa – zwłaszcza jego cyfrowej odmiany, czyli cyberbezpieczeństwa.

Należy wskazać, że płaszczyzna międzynarodowa stanowi niezbędny wymiar ochrony praw człowieka, gdyż to w niej są tworzone nowe standardy w dziedzinie praw człowieka, które są następnie wnoszone do systemu prawa wewnętrznego i praktyki państw. Z drugiej strony, istnienie regulacji prawnomiędzynarodowych jest w coraz większej mierze gwarancją efektywności systemów prawa wewnętrznego. Instytucje międzynarodowe stają się często instancją odwoławczą dla jednostek oraz środkiem nacisku na rządy krajów nieprzestrzegających podstawowych praw i wolności człowieka. Poparcie dla jednostek, społeczności czy narodów walczących o swoje prawa, ich sukcesy w tej walce czynią jeden z elementów kształtowania nowego, demokratycznego porządku międzynarodowego.

Słowa kluczowe: wolność słowa, cyberbezpieczeństwo, media cyfrowe, regulacja, prawo międzynarodowe

Marek Pawlik*
Ewa Niewiadomska-Szynkiewicz**

Rola centrów wymiany i analizy informacji w budowaniu odporności kluczowych sektorów polskiej gospodarki

Streszczenie

W ostatnich latach obserwuje się lawinowy wzrost zagrożeń z cyberprzestrzeni zarówno systemów informacyjnych (systemów IT), jak i cyfrowych systemów eksploatacyjnych (systemów OT) wykorzystujących technologie informacyjne i komunikacyjne (technologie ICT). Jednocześnie rośnie ilość gromadzonych, przetwarzanych i udostępnianych cyfrowych danych. Dostępność tych danych istotnie wpływa na rozwój gospodarczy kraju, wspiera funkcjonowanie administracji państwa, podnosi poziom obronności, ochrony zdrowia, edukacji. W tej sytuacji podstawowego znaczenia nabiera budowanie świadomości ryzyk i nabywanie umiejętności zabezpieczania sieci, systemów i cyfrowych usług przed cyberzagrożeniami. Ważną rolę w tym zakresie odgrywają nowego typu struktury, tzw. centra wymiany i analizy informacji (ISAC). Współautorzy na podstawie zapisów prawa i własnych doświadczeń związanych z funkcjonowaniem ISAC-Kolej i ISAC-GIG przedstawiają ekosystem dookoła ISAC, zadania tych struktur oraz stojące przed nimi wyzwania.

Słowa kluczowe: cyberbezpieczeństwo, operatorzy usług kluczowych, centra wymiany i analizy informacji, ISAC

* Dr hab. inż. Marek Pawlik, prof. Instytutu Kolejnictwa, zastępca dyrektora ds. interoperacyjności kolei, Instytut Kolejnictwa w Warszawie, e-mail: mpawlik@ikolej.pl, ORCID: 0000-0003-3357-7706.

** Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz, kierownik Zespołu Złożonych Systemów, Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, doradca dyrektora w Głównym Instytucie Górnictwa (GIG), zastępca przewodniczącego ISAC-GIG, e-mail: ewa.szynkiewicz@pw.edu.pl, ORCID: 0000-0003-4782-3816.

Wstęp

Technologie ICT, czyli technologie informacyjne i komunikacyjne (ang. Information and Communication Technologies), są obecne w wielu obszarach gospodarki, chociaż znaczna część społeczeństwa może nie zdawać sobie z tego sprawy. Dla wielu obywateli jest oczywiste, że cyfrowe usługi funkcjonują w sektorze finansowym, administracji centralnej i lokalnej państwa, a od czasu pandemii umożliwiają pracę i naukę zdalną. Prawdopodobnie niewiele osób zdaje sobie sprawę jak ważną rolę odgrywają technologie ICT we wspieraniu i realizacji usług transportowych, dostarczaniu wody pitnej, zapewnianiu i rozliczaniu energii elektrycznej czy w ochronie zdrowia. Obecnie bezpieczeństwo państw i ich obywateli w znacznym stopniu zależy od dostępności i kompetencji personelu oraz systemów i narzędzi programistycznych, które chronią kluczowe usługi cyfrowe we wszystkich warstwach systemów ICT, od warstwy fizycznej po warstwę aplikacji. Niestety, nawet wśród pracowników zajmujących się technologiami informacyjnymi obserwuje się stosunkowo niski poziom wiedzy na temat warstw systemów ICT oraz świadomości, w jaki sposób warstwy te ze sobą współpracują. Budowanie i utrzymywanie systemów zabezpieczeń przed cyberzagrożeniami, które mogą atakować na różnych poziomach wymiany i przetwarzania danych w systemach ICT, wymaga wiedzy i stałego podnoszenia kompetencji pracowników ważnych dla bezpieczeństwa państwa podmiotów. Braki lub luki w zabezpieczeniach przyczyniają się do łatwego rozprzestrzeniania się zagrożeń. Atakowane są kolejne instytucje i organizacje w poszczególnych branżach, pokonywane są bariery organizacyjne, cyberataków dotykają również jednostki z innych obszarów działalności. Atak na system egzaminowania kierowców może np. spowodować wstrzymanie pracy grupy placówek medycznych. Przyczyna może być oczywista, np. wykorzystywanie wspólnego centrum przetwarzania danych. Może być też trudna do wykrycia, np. atak w jednej z warstw wymiany danych przekazywanych siecią światłowodową. Wspomaganie podmiotów korzystających z rozwiązań cyfrowych do identyfikacji zagrożeń, budowania umiejętności cyfrowych pracowników, wdrażania i utrzymywania zabezpieczeń to zadania centrów wymiany i analiz informacji (ISAC), których działalności jest poświęcony niniejszy artykuł.

Lista podmiotów zobowiązanych do identyfikowania zagrożeń i przeciwdziałania zagrożeniom oraz raportowania incydentów bezpieczeństwa

W 2016 roku Parlament Europejski przyjął dyrektywę na rzecz wspólnego wysokiego bezpieczeństwa sieci i systemów[1]. Angielskie określenie sieci i systemów (network and information systems) jest wykorzystywane do szybkiego i niebudzącego wątpliwości identyfikowania tej dyrektywy jako dyrektywy NIS. Do polskiego porządku prawnego została ona wprowadzona w 2018 roku ustawą o krajowym systemie cyberbezpieczeństwa[2], identyfikowaną jako ustawa KSC. Zarówno dyrektywa NIS, jak i ustawa KSC wybierają grupy podmiotów, spośród których właściwe władze krajowe wskazują tzw. operatorów usług kluczowych. Podmioty te są zobowiązane do identyfikowania cyfrowych zagrożeń, zabezpieczania się przed nimi i raportowania incydentów. Sektor integrujący podmioty odpowiedzialne za pozyskiwanie i dostarczanie energii, w tym energii elektrycznej, podzielono na aż siedem podsektorów. Podsektory oraz odpowiadające im zakresy działań przedstawiono w tabeli 1. Za kluczowe uznano również usługi transportowe. W sektorze transportu wyróżniono cztery podsektory odpowiadające czterem rodzajom transportu, tj.: lotniczy, kolejowy, wodny i drogowy. Podmioty, z których są wskazywani operatorzy usług kluczowych w transporcie, zestawiono w tabeli 2.

Tabela 1. Operatorzy usług kluczowych w sektorze „energia"

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
Energia	wydobywanie kopalin	wydobywanie: gazu ziemnego, ropy naftowej, węgla brunatnego, węgla kamiennego oraz pozostałych kopalin
	energia elektryczna	wytwarzanie energii elektrycznej, przesyłanie energii elektrycznej, dystrybucja energii elektrycznej, obrót energią elektryczną, przetwarzanie albo magazynowanie energii elektrycznej, świadczenie usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną
	ciepło	wytwarzanie ciepła, obrót ciepłem, przesyłanie ciepła, dystrybucja ciepła

1 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194/1.

2 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
	ropa naftowa	wytwarzanie paliw ciekłych, przesyłanie ropy naftowej, przesyłanie paliw ciekłych siecią rurociągów, magazynowanie ropy naftowej, w tym bezzbiornikowego podziemnego magazynowania ropy naftowej, przeładunek ropy naftowej, magazynowanie paliw ciekłych, bezzbiornikowe podziemne magazynowanie paliw ciekłych, przeładunek paliw ciekłych, obrót paliwami ciekłymi, obrót paliwami ciekłymi z zagranicą, wytwarzanie paliw syntetycznych
	gaz	wytwarzanie paliw gazowych, przesyłanie paliw gazowych, obrót gazem ziemnym z zagranicą, obrót paliwami gazowymi, operator systemu przesyłowego gazowego, operator systemu dystrybucyjnego gazowego, operator systemu magazynowania paliw gazowych, operator systemu skraplania gazu ziemnego
	dostawy usług w sektorze energii	dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii
	jednostki nadzorowane i podległe	jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane, jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Tabela 2. Operatorzy usług kluczowych w sektorze „transport"

Sektor	Podsektor	Rodzaje podmiotów/rodzaje działalności
Transport	lotniczy	przewoźnik lotniczy, zarządzający lotniskiem, przedsiębiorca wykonujący określone usługi i/lub zadania związane z kontrolą bezpieczeństwa przewoźników lotniczych oraz innych użytkowników statków powietrznych, instytucja zapewniająca służby żeglugi powietrznej
	kolejowy	zarządcy infrastruktury kolejowej (z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, prywatnej i wąskotorowej), przewoźnicy kolejowi
	wodny	armatorzy w transporcie morskim pasażerów i towarów, armatorzy w żegludze śródlądowej, podmioty zarządzające portami i przystaniami morskimi, podmioty zarządzające obiektami portowymi, podmioty prowadzące na terenie portów działalność wspomagającą transport morski, służby kontroli ruchu statków (VTS)
	drogowy	zarządcy dróg, podmioty realizujące usługi ITS

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Tabela 3. Operatorzy usług kluczowych w obszarze finansów, zdrowia, wody i infrastruktury cyfrowej

Sektor	Rodzaje podmiotów/rodzaje działalności
Bankowość i infrastruktura rynków finansowych	instytucje kredytowe, banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, spółdzielcze kasy oszczędnościowo-kredytowe, podmioty prowadzące rynek regulowany, CCP – osoby prawne działające w obrocie na rynku finansowym będące nabywcą dla sprzedawcy i sprzedawcą dla nabywcy, podmioty zależne krajowego depozytu uczestniczące w obsłudze depozytu papierów wartościowych
Ochrona zdrowia	podmioty lecznicze, jednostki właściwe w zakresie systemów informacyjnych ochrony zdrowia, Narodowy Fundusz Zdrowia, działy farmacji szpitalnej, apteki szpitalne, hurtownie farmaceutyczne, podmioty wprowadzające do obrotu produkty lecznicze, importerzy produktów leczniczych/substancji czynnych, wytwórcy produktów leczniczych/substancji czynnych, importerzy równolegli, dystrybutorzy substancji czynnych, ogólnodostępne apteki
Zaopatrzenie w wodę pitną	przedsiębiorstwa wodociągowo-kanalizacyjne
Infrastruktura cyfrowa	podmioty świadczące usługi DNS, podmioty prowadzące punkty wymiany ruchu internetowego (IXP), podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD)

Źródło: Na podstawie ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa...

Ustawa o krajowym systemie cyberbezpieczeństwa zgodnie z dyrektywą NIS wskazuje także podmioty, które odgrywają rolę operatorów usług kluczowych w czterech kolejnych sektorach. Są to instytucje oferujące usługi bankowe i finansowe, ochrony zdrowia, zapewnienia wody pitnej i infrastruktury cyfrowej. Podobnie jak dla sektorów energii i transportu podano rodzaje podmiotów oraz działalności, które upoważniają właściwy organ krajowy do wskazywania, decyzjami administracyjnymi, podmiotów będących operatorami usług kluczowych i tym samym zobowiązanych do realizacji związanych z tym zadań.

Rozszerzona lista podmiotów zobowiązanych do identyfikowania zagrożeń i przeciwdziałania zagrożeniom oraz raportowania incydentów bezpieczeństwa

Wskazane w tabelach 1–3 podmioty nie wyczerpują katalogu instytucji i przedsiębiorstw, których działalność jest kluczowa dla funkcjonowania państwa i jego obywateli, których wszelkie zakłócenia w ich pracy mogą skutkować

bardzo poważnymi konsekwencjami. Intensywne ataki, z jakimi mają obecnie do czynienia państwa demokratyczne, w tym państwa członkowskie Unii Europejskiej, spowodowały, że w grudniu 2022 roku Parlament Europejski przyjął dyrektywę NIS-2[3]. Powiększa ona katalog podmiotów o operatorów systemów chłodniczych oraz operatorów instalacji wodorowych jako nowego rodzaju paliwa. Uwzględnia także przedsiębiorstwa zbierające, odprowadzające i oczyszczające ścieki. Dodatkowo do listy podmiotów obsługujących cyfrową infrastrukturę dołączono dostawców usług chmurowych, centra przetwarzania danych, sieci dostarczania treści, usługi zaufania, publiczne i publicznie dostępne usługi łączności elektronicznej oraz podmioty oferujące usługi ICT pomiędzy różnymi przedsiębiorstwami. Uwzględniono także instytucje administracji publicznej gromadzące i przetwarzające dane wrażliwe oraz operatorów naziemnej infrastruktury związanej z przestrzenią kosmiczną.

Oprócz sektorów kluczowych dyrektywa NIS-2 definiuje także sektory ważne z punktu widzenia cyberbezpieczeństwa. Zaliczono do nich usługi pocztowe i kurierskie, gospodarowanie odpadami, produkcję, wytwarzanie i dystrybucję chemikaliów, produkcję, przetwarzanie i dystrybucję żywności, produkcję wyrobów medycznych, komputerów, wyrobów elektronicznych i optycznych, urządzeń elektrycznych, maszyn i urządzeń, pojazdów i pozostałego sprzętu transportowego, a także dostawców usług cyfrowych, w tym dostawców internetowych platform handlowych, wyszukiwarek internetowych, platform usług sieci społecznościowych oraz podmioty zaangażowane w badania naukowe.

Dyrektywa NIS-2 diametralnie zmieniła sytuację przedsiębiorstw działających w poszczególnych sektorach. Dotychczas status operatorów usług kluczowych był nadawany przedsiębiorstwom decyzją administracyjną właściwych władz krajowych. Po wejściu w życie dyrektywy NIS-2 status taki, zgodnie z zapisami dyrektywy, z mocy prawa uzyskają podmioty publiczne i prywatne działające w sektorach kluczowych i/lub sektorach ważnych, które kwalifikują się jako średnie przedsiębiorstwa zgodnie z zaleceniem 2003/361/WE[4] lub większe oraz świadczą usługi i/lub prowadzą działalność na terenie Unii

3 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Tekst mający znaczenie dla EOG), Dz. Urz. UE 2022, L 333/80.

4 Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. dotyczące definicji przedsiębiorstw mikro, małych i średnich (notyfikowane jako dokument nr C(2003) 1422), ibidem 2003, L 124.

Europejskiej. Podsumowując, wszystkie podmioty działające w sektorach kluczowych i sektorach ważnych, z wyłączeniem tych, które zatrudniają mniej niż 50 osób i mają obroty roczne i/lub roczną sumę bilansową nieprzekraczającą 10 mln euro, z mocy prawa będą zobowiązane do realizacji zadań przeciwdziałających cyberzagrożeniom. W ten sposób wiele podmiotów stanie się z mocy prawa operatorami usług kluczowych. Będą one zobowiązane nie tylko do wykrywania zagrożeń, kształtowania kompetencji pracowników w zakresie cyberbezpieczeństwa oraz wdrażania i utrzymywania zabezpieczeń, ale także do samodzielnego identyfikowania świadczonych przez siebie usług kluczowych, które dotychczas były wskazywane w decyzjach administracyjnych. Rozsądne podejmowanie decyzji w tym zakresie wymaga nie tylko przeglądu wszystkich cyfrowych rozwiązań oraz zapewnianych przez nie usług, lecz także określania możliwych konsekwencji różnego rodzaju cyberataków na te usługi.

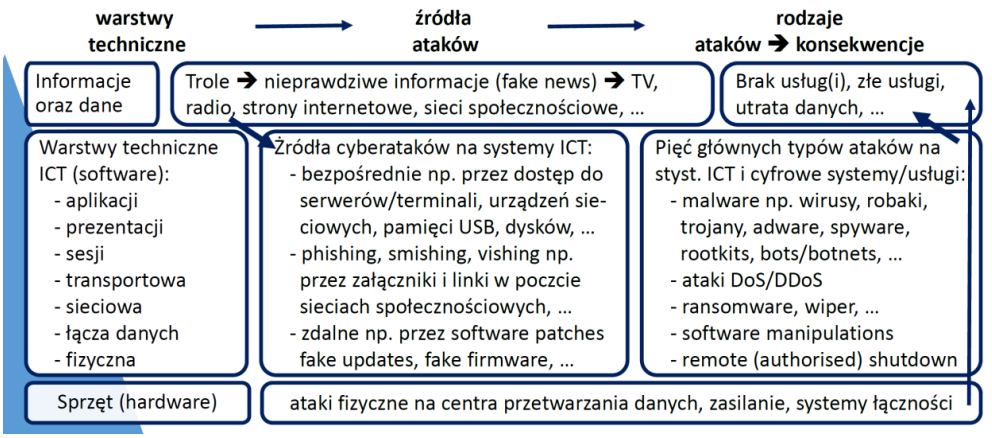
Centra wymiany i analizy informacji działające w Polsce

Zgodnie z wymaganiami dyrektywy NIS polska ustawa o krajowym systemie cyberbezpieczeństwa definiuje zespoły reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (ang. Computer Security Incident Response Teams – CSIRT). W Polsce działają trzy CSIRT-y: CSIRT GOV, CSIRT MON oraz CSIRT NASK. Ustawa zawiera także wiele zapisów na temat tzw. sektorowych zespołów cyberbezpieczeństwa, przy czym nie ma w niej wytycznych dotyczących struktur typu CERT, takich jak SOC i NOC oraz struktur typu ISAC. Zespoły CERT (ang.Computer Emergency Response Team) zajmują się reagowaniem na incydenty komputerowe, obserwacją i analizą określonych aplikacji, usług cyfrowych, a także części cyfrowej infrastruktury, SOC (ang. Security Operations Centers) to centrum monitorowania bezpieczeństwa aplikacji i usług, a NOC (ang. Network Operations Centers) to centrum monitorowania bezpieczeństwa sieci. Zespoły takie jako CERT-y pracują w trybie 24/7 i zatrudniają wyspecjalizowany personel. Zupełnie inną funkcję pełnią ISAC (ang. Information Sharing and Analysis Centre). Centra wymiany i analizy informacji są tworzone w celu wymiany wiedzy i doświadczeń na temat incydentów cyberbezpieczeństwa w różnych sektorach gospodarki. Ich historia sięga lat 90. ubiegłego wieku. Idea zrodziła się w Stanach Zjednoczonych Ameryki w związku z raportem tzw. Prezydenckiej Komisji ds. Zabezpieczenia Infrastruktury Krytycznej (ang. President's Commission on Critical Infrastructure Protection – PCCIP). W raporcie tym wskazano internet i cyfrowe

systemy komunikacyjne jako najpoważniejsze zagrożenie dla infrastruktury krytycznej państwa. Pierwsze ISAC powstały po atakach terrorystycznych w Stanach Zjednoczonych i od tamtego czasu tworzone są kolejne w różnych częściach świata. Centra są miejscem wymiany informacji i doświadczeń na temat cyberbezpieczeństwa pomiędzy publicznymi i prywatnymi podmiotami funkcjonującymi w tym samym obszarze gospodarki lub powiązanych obszarach. Funkcję taką w sektorze usług bankowych i finansowych pełni Komisja Nadzoru Finansowego (KNF). W obszarze transportu kolejowego od grudnia 2020 roku – ISAC-Kolej, a w sektorze wydobywczo-energetycznym utworzony w 2022 roku ISAC-GIG. Autorzy artykułu uczestniczą w pracach ISAC-Kolej i ISAC-GIG. Podstawą ich działalności jest dobrowolna współpraca podmiotów różnej wielkości i o różnym charakterze, których łączy wykorzystywanie cyfrowych rozwiązań w tym samym lub współpracujących sektorach/podsektorach/obszarach działalności. Część z nich to duże przedsiębiorstwa dysponujące własnymi zasobami obejmującymi infrastrukturę i kompetentną kadrę, zapewniającymi wykrywanie cyberzagrożeń i im przeciwdziałanie. Pozostali członkowie to niewielkie podmioty, które nie mają takich zasobów. Cel jest wspólny – budowanie wiedzy i umiejętności w zakresie ochrony sieci, systemów i usług u wszystkich partnerów, bez względu na ich wielkość i zakres działania. Incydenty bezpieczeństwa i ataki dotykają wszystkich, szybko się rozprzestrzeniają, przenikają między różnymi podmiotami w branży, a nawet pomiędzy branżami.

Misja i zadania ISAC

Obecnie ISAC wspierają podmioty, które już zostały uznane za operatorów usług kluczowych oraz podmioty, które mimo że nie mają formalnie nadanego takiego statusu, zdają sobie sprawę z przynajmniej części cyfrowych zagrożeń i podejmują działania na rzecz cyberbezpieczeństwa. Budują niezbędne kompetencje i przygotowują się do spełnienia przyszłych wymagań formalnych. Mając świadomość cyberzagrożeń i wynikających z nich konsekwencji, dobrowolnie wprowadzają kolejne zabezpieczenia. Należy pamiętać, że skuteczna ochrona przed cyberzagrożeniami wymaga identyfikacji potencjalnych incydentów bezpieczeństwa i ataków oraz informacji na temat wykorzystywanych systemów ICT i ich otoczenia. Powiązania między cyberzagrożeniami oraz systemami ICT i ich otoczeniem przedstawia rysunek 1.



Źródło: Opracowanie własne.

Rys. 1. Środowisko cyberataków i ataków długoterminowych (typu APT)

Systemy infrastruktury krytycznej działają tylko wtedy, kiedy jest dostępna właściwa infrastruktura taka, jak: centra przetwarzania danych (CPD), infrastruktura energetyczna zapewniająca ich zasilanie i telekomunikacyjna zapewniająca łączność pozwalającą na wymianę danych pomiędzy geograficznie rozproszonymi na dużych obszarach cyfrowymi urządzeniami. Znaczenie infrastruktury krytycznej pokazują obserwowane w ostatnich latach zmasowane ataki. Widać to doskonale na przykładzie objętej wojną Ukrainy – to ataki na elektrownie, sieci przesyłowe czy maszty telekomunikacyjne. Zabezpieczanie tej infrastruktury i odtwarzanie jej po zniszczeniach to zadania dla wojska oraz służb energetycznych i telekomunikacyjnych. Z punktu widzenia ISAC infrastruktura taka ma po prostu być dostępna.

Z drugiej strony obserwuje się intensyfikację działań, których celem jest dezinformacja. Tak zwane farmy trolli tworzą i rozpowszechniają na szeroką skalę całkowicie nieprawdziwe lub zmanipulowane informacje oraz przekłamane dane, tzw. fake newsy, starając się w ten sposób budować fałszywy, sprzyjający określonym państwom lub grupom interesu przekaz medialny. Działania ISAC nie koncentrują się na wymianie i udostępnianiu informacji. Organizacje te zajmują się tym, co jest pomiędzy warstwą infrastruktury krytycznej, warstwą udostępniania i wymiany informacji oraz danych, w której stosowane są systemy cyfrowe wykorzystujące technologie ICT. Celem są działania, których rezultatem jest podnoszenie świadomości o potencjalnych zagrożeniach oraz wzmacnianie zabezpieczeń przed cyberzagrożeniami we wspieranych przez nie podmiotach.

Pojedynczy haktywiści[5], skrypt krakerzy[6] i hakerzy, a także coraz częściej i w coraz większej skali grupy hakerskie sponsorowane przez struktury mafijne, wojskowe czy państwowe atakują systemy ICT oraz cyfrowe usługi i urządzenia. Zazwyczaj wykorzystują do tego celu:

– **nieuprawniony bezpośredni dostęp** do serwerów i/lub terminali systemów ICT, urządzeń sieciowych w szczególności tych z niezabezpieczonymi spam portami. Podłączają do nie swoich komputerów, drukarek i innych urządzeń sieciowych zainfekowane pamięci USB czy zainfekowane dyski zewnętrzne. Wykorzystują inne systemy i urządzenia pozwalające na bezpośrednie przekazywanie złośliwego kodu, np. przez urządzenia korzystające z technologii bezprzewodowych takich jak WiFi czy bluetooth;

– **socjotechniki**, w tym fałszywe strony www, wiadomości e-mail z zainfekowanymi załącznikami lub linkami do specjalnie spreparowanych stron podszywających się pod strony popularnych serwisów, banków czy usługodawców (tzw. phishing). Wiadomości wymieniane między urządzeniami mobilnymi w formie SMS, MMS oraz w komunikatorach, z linkami do specjalnie tworzonych fałszywych stron www wprowadzających w błąd i/lub infekujących urządzenia nieostrożnych użytkowników (tzw. smishing). Głosowe namawianie na instalowanie aplikacji udostępniających atakującym zdalny dostęp do urządzeń (tzw. vishing);

– **nieuprawniony lub szkodliwie wykorzystywany zdalny dostęp** do systemów, wirtualnych serwerów, wirtualnych sieci prywatnych, kopii zapasowych systemów i danych oraz urządzeń przez instalowanie cyfrowych łat ze złośliwym kodem (tzw. fakepatches), fałszywe uaktualnienia (tzw. fakeupdaates), oprogramowanie sprzętowe podszywające się pod prawdziwy firmware (tzw. fakefirmware), które swoim działaniem może szpiegować użytkowników, blokować systemy i usługi lub nawet fizycznie niszczyć urządzenia.

Ataki na systemy ICT oraz cyfrowe usługi i urządzenia powodują materializację cyfrowych ryzyk opisanych na zlecenie Komisji Europejskiej przez ekspertów do spraw cyberbezpieczeństwa. Opis tych grup zawiera m.in.

5 Haktywiści – osoby, które używają komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji.

6 Skrypt krakerzy – osoby, które używają programów i skryptów napisanych przez innych bez dogłębnej znajomości zasad ich działania, jedynie po to, żeby uzyskać nieuprawniony dostęp do komputerowych kont użytkowników lub plików albo przeprowadzać ataki na systemy komputerowe.

„Transport cybersecurity toolkit”[7]. Zdefiniowano w nim cztery główne typy zagrożeń, tj.:

– **złośliwe oprogramowanie** obejmujące wirusy, robaki, trojany, adware, spyware, keyloggers, rootkits, bots & botnets itd., łącznie określane jako malware;

– generowanie **lawiny zapytań do systemów, stron www, cyfrowych usług** w wersji prostej (**ataki DoS**) i w wersji rozproszonej, tj. wykorzystującej wiele źródeł zapytań (np. z wykorzystaniem tożsamości uzyskanych poprzez phishing) **ataki DDoS** skutkujące blokowaniem lub zniszczeniem zaatakowanych usług cyfrowych;

– **nieuprawniony dostęp i kradzież danych** przez eksport danych lub ich szyfrowanie w celu wymuszenia korzyści majątkowych dzięki okupom (tzw. ransomware) lub **usuwanie danych** z wykorzystaniem tzw. wiperów. W tym drugim przypadku celem atakującego jest zazwyczaj zniszczenie systemu teleinformatycznego, np. w związku z działaniami zbrojnymi;

– **manipulacje oprogramowaniem** polegające na pozyskaniu ekspertów od dostawców systemów bądź wielomiesięcznym podsłuchiwaniu i analizowaniu działania systemów (tzw. ataki APT) w celu wytworzenia i wprowadzenia do systemu własnych urządzeń lub użytkowników, którzy mając złośliwe zamiary i wydając groźne polecenia, będą traktowani przez system jako w pełni uprawnieni użytkownicy. Takie ataki są trudne do realizacji, ale prowadzą do spektakularnych „zwycięstw” atakujących, np. katastrof.

Wojna za wschodnią granicą Polski pokazała, że do głównych zagrożeń dodać należy jeszcze **wyłączenie systemu lub urządzenia na odległość** [ang. remote (authorised) shutdown – RaS], które to działanie nie jest rozpoznane przez wyłączającego jako nieuprawnione. W wyniku prac prowadzonych w Instytucie Kolejnictwa wskazano kilka takich przypadków. Dotyczyły one m.in. skradzionych w Ukrainie i wywiezionych na wschód maszyn rolniczych czy linii automatycznego butelkowania win krymskich, która została wyłączona na odległość przez europejskiego producenta linii. W tym kontekście nowego znaczenia nabiera pytanie o to, kto jest producentem systemów, względnie kto i w jakim kraju przygotował i wgrał firmware.

7 *Transport cybersecurity toolkit*, European Union, 2020, https://www.fecc.org/wp-content/uploads/2020/12/DG-MOVE-Transport-Cybersecurity-Toolkit-FINAL.pdf [dostęp: 5.12.2022].

Polskie ISAC i zakres ich działania

W Polsce struktury typu ISAC nie pracują w trybie 24/7. Ich zadaniem jest wspomaganie już ustanowionych i przyszłych operatorów usług kluczowych. Działania koncentrują się na wymianie informacji pomiędzy podmiotami. Wymianą informacji, kompetencji i dobrych praktyk jest zainteresowanych wiele jednostek. Znacznie gorzej wygląda sprawa finansowania działalności ISAC. Ewentualny rozdział kosztów na podmioty jest poważnym wyzwaniem. Można wprawdzie założyć, że działania ISAC będą finansowane ze źródeł zewnętrznych, ale ich pozyskanie wymaga czasu i, niestety, dodatkowych środków. Dlatego członkowie ISAC-Kolej podjęli decyzję, że każdy podmiot przystępujący do ISAC, począwszy od założycieli, w pełni pokrywa koszty swojego zaangażowania we wspólne prace. Obecnie w podobnej formule funkcjonuje ISAC-GIG. W efekcie oba centra korzystają z wymiany informacji drogą elektroniczną i spotkań on-line. ISAC-Kolej nie ma ambicji przekształcić się w przyszłości w strukturę typu CERT, niezależnie od tego, że w wielu publikacjach wskazuje się przekształcenie struktur typu ISAC w struktury typu CERT jako naturalną konsekwencję rozwoju zabezpieczeń przed cyberzagrożeniami na poziomie branż czy sektorów. W transporcie kolejowym struktury typu CERT już działają, współpracują z branżowym centrum ISAC, i wydaje się niemal pewne, że będą się rozwijać równolegle do ISAC-Kolej. ISAC-GIG nie wyklucza budowy sektorowego SOC. Takie struktury funkcjonują u niektórych partnerów, ale mają one zasięg lokalny.

Jak ISAC wspierają swoich członków

ISAC-Kolej nie tworzy samodzielnie dużych opracowań o stanie cyberbezpieczeństwa sektora transportu. Dzieli się informacjami zarówno pozyskanymi z opracowań zewnętrznych, jak i z raportów przygotowanych przez swoich członków. Przykładem w obszarze transportu kolejowego mogą być przeznaczone dla kolei raporty Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[8] opracowane we współpracy z Agencją UE ds. Kolei (ERA), które nie

8 *Railway Cybersecurity, security measures in the Railway Transport Sector*, European Union Agency for Cybersecurity ENISA, November 2020, https://cyberpolicy.nask.pl/wp-content/uploads/2021/01/ENISA-Report-Railway-Cybersecurity.pdf [dostep: 25.01.2023]; *Railway Cybersecurity. Good practices in cyber risk management*, European Union Agency for

są dostępne w języku polskim, a były szczegółowo omawiane i dyskutowane na forum ISAC-Kolej. Podobnie były dyskutowane dokumenty normatywne dotyczące cyberbezpieczeństwa w transporcie kolejowym, np. specyfikacja techniczna CENELEC TS 50701[9] czy tom standardów kolejowych Centralnego Portu Komunikacyjnego (CPK) dotyczący spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa[10]. Omawiane i dyskutowane były także dokumenty prawne. W efekcie zostały zgłoszone uwagi zarówno do projektu dyrektywy NIS-2, jak i do specyfikacji TS 50701.

Na potrzeby podmiotów kolejowych podczas prac ISAC-Kolej zostały przyjęte wytyczne dotyczące cyberbezpieczeństwa pracowników tych podmiotów. Wytyczne zostały udostępnione nie tylko członkom ISAC, lecz także wszystkim zainteresowanym poprzez druk w „Problemach Kolejnictwa"[11] oraz „Magazynie Kultury Bezpieczeństwa"[12] wydawanym przez Urząd Transportu Kolejowego. Co istotniejsze, członkowie ISAC-Kolej drogą elektroniczną regularnie otrzymują:

– codzienne raporty CSIRT GOV dotyczące złośliwego ruchu sieciowego (rekomendacje dotyczące blokowania konkretnych IP);

– tygodniowe raporty CSIRT GOV zawierające informacje na temat wykrytych podatności w produktach IT (rekomendacje dotyczące aktualizacji systemów i oprogramowania);

– tygodniowy „Biuletyn Informacyjny" SOC PKP Informatyka dotyczący cyberbezpieczeństwa w transporcie kolejowym.

W przypadkach wykrycia zagrożeń:

– informacje o nowych kampaniach phishingowych;

– informacje o zarejestrowaniu domen, które mogą być wykorzystane do ataków phishingowych (rekomendacje blokowania złośliwych domen na

Cybersecurity ENISA, November 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management [dostęp: 25.01.2023]; *Zoning and conduits for railways*, European Union Agency for Cybersecurity ENISA and European Rail ISAC, February 2022, https://www.enisa.europa.eu/publications/zoning-and-conduits-for--railways [dostęp: 25.01.2023].

9 CENELEC Technical Specification TS 50701, Railway applications – Cybersecurity, 2021.

10 *Standardy techniczne. Szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego. Wytyczne projektowania*, *t. 18*, *Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa*, wersja 1.3.0, Warszawa 2021.

11 M. Pawlik, *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*, „Problemy Kolejnictwa" 2021, z. 191.

12 Idem, *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych* [w:] *Magazyn kultury bezpieczeństwa*, Warszawa 2021, s. 45–53.

urządzeniach brzegowych, stosowania odpowiednich filtrów antyspamowych, czujności przy wysyłaniu/odbieraniu wiadomości przesyłanych drogą elektroniczną przez pracowników);

– informacje o wykryciu podatności zero-day, możliwości ich wykorzystania oraz IoC (rekomendacje – różne, w zależności od typu podatności);

– informacje o kampaniach phishingowych dystrybuujących złośliwe oprogramowanie oraz IoC złośliwej kampanii (rekomendacje – wdrożenie stosownych reguł na urządzeniach filtrujących pocztę elektroniczną),

a w razie stwierdzenia – informacje o atakach DDoS, w tym o możliwych atakach na strony internetowe i serwisy (rekomendacje – ochrona antyDDoS, monitorowanie infrastruktury, przygotowanie się na ograniczenia ruchu przy eskalacji), oraz w razie konieczności – przydatne informacje, np. dotyczące certyfikacji produktów IT na terenie Rosji, działalności grup APT, Killnet itp.

Budowie ISAC-GIG przyświecała potrzeba wymiany wiedzy, doświadczeń oraz dobrych praktyk w zakresie stosowania zabezpieczeń systemów teleinformatycznych, a także współdziałania w obsłudze incydentów dotyczących cyberbezpieczeństwa w sektorach wydobywczym i energetycznym. W skład ISAC-GIG wchodzą główni przedstawiciele zakładów wydobywczych, w tym podziemne zakłady górnicze węgla kamiennego i miedzi, dostawcy energii, firmy wspierające górnictwo oraz jednostki naukowe, tj. instytuty badawcze oraz uczelnie wyższe. Do głównych zadań ISAC-GIG należy:

– umożliwienie aktywnego uczestnictwa podmiotom z sektora wydobywczego i energetycznego w krajowym systemie cyberbezpieczeństwa oraz dostępu do aktualnych informacji dotyczących bezpieczeństwa;

– wymiana doświadczeń, budowanie świadomości cyfrowej oraz rozwój kompetencji w dziedzinie cyberbezpieczeństwa (szkolenia, warsztaty, działania proaktywne);

– wymiana informacji na temat rodzajów stosowanych zabezpieczeń oraz struktur cyberbezpieczeństwa w organizacjach członkowskich ISAC-GIG;

– wsparcie w zakresie cyberbezpieczeństwa zaangażowanych podmiotów zgodnie z wymogami ustawy o krajowym systemie cyberbezpieczeństwa;

– wsparcie technologiczne w zakresie ciągłości działania systemów IT/OT/IoT;

– wypracowanie wytycznych dotyczących stosowania rozwiązań do ochrony przed zagrożeniami z sieci;

– określanie wymagań dotyczących certyfikacji cyberbezpieczeństwa produktów i usług w sektorach wydobywczym i energetycznym.

Do wymiany informacji na temat wskaźników zagrożeń i złośliwego oprogramowania w ISAC-GIG jest wykorzystywana platforma MISP (Malware Information Sharing Platform & Threat Sharing). Korzysta z niej wiele organizacji na świecie, a jej celem jest wspieranie prac na rzecz przeciwdziałania ukierunkowanym atakom oraz ich wczesnej detekcji. Na stronie domowej ISAC-GIG (https://isac.gig.eu) dostępne są informacje o bieżącej aktywności centrum i działaniach partnerów na rzecz cyberbezpieczeństwa. Będą na niej również udostępniane zbiorcze raporty roczne na temat cyberbezpieczeństwa w sektorze wydobywczo-energetycznym.

W ramach swojej dotychczasowej działalności ISAC-GIG i wchodzące w jego skład jednostki organizują regularne cyberpoligony, które dzięki rywalizacji zespołów bezpieczeństwa poszczególnych partnerów sprawdzają swoją wiedzę i umiejętności w zakresie reagowania na incydenty i zwalczania cyberataków. Organizowane są również warsztaty na konferencjach branżowych oraz seminaria, których celem jest podnoszenie poziomu świadomości cyberzagrożeń dotykających sektor oraz przekazywanie wiedzy o trendach i najnowszych rozwiązaniach w wykrywaniu cyberataków i ograniczaniu ich skutków. Prelegentami są naukowcy oraz przedstawiciele firm ICT. ISAC-GIG był inicjatorem oraz współorganizatorem utworzenia na Politechnice Śląskiej studiów podyplomowych z dziedziny cyberbezpieczeństwa systemów przemysłowych. W planach jest organizacja regularnych szkoleń z cyberbezpieczeństwa dla pracowników sektora.

Współpraca członków ISAC-GIG z środowiskiem naukowym zaowocowała pozyskaniem finansowania na projekt badawczy, którego celem jest opracowanie i wytworzenie nowych systemów typu SOAR wyposażonych w autorskie narzędzia sprzętowo-programowe do wykrywania anomalii w sieciach IT/OT/IoT, w tym wykorzystujące metody sztucznej inteligencji. Planuje się, że w przyszłości mogłyby one wspierać sektorowy SOC. Podmioty członkowskie ISAC-GIG planują w przyszłości dalsze wnioskowanie do krajowych i międzynarodowych jednostek finansujących badania o fundusze na prace związane z wytwarzaniem innowacyjnych rozwiązań w dziedzinie cyberbezpieczeństwa.

Zakończenie

To początek drogi. Polskie ISAC to młode organizmy, które dopiero się kształtują i ciągle poszukują najlepszej drogi dla siebie. Stoi przed nimi wiele wyzwań, w tym taka organizacja współpracy z podmiotami dostarczającymi technologie

cyfrowe, żeby nie zostały naruszone równe zasady konkurencji pomiędzy dostawcami sprzętu i oprogramowania. Tego typu firmy nie są wprost zapraszane do udziału w pracach ISAC. Formuła współpracy musi być pilnie wypracowana.

Konieczna jest również intensyfikacja współpracy między partnerami centrów, budowanie wzajemnego zaufania i przekonania, że działając razem, można osiągnąć znacznie więcej. Z czasem mogą pojawić się potrzeby inwestycji, np. w sprzęt i oprogramowanie do tworzenia platform szkoleniowych, ale o tym będą już indywidualnie decydować poszczególne centra. Następnym krokiem będzie z pewnością większe otwarcie na otoczenie, nie tylko w ramach reprezentowanego sektora, ale też na lokalną społeczność, przedsiębiorców i instytucje administracji państwa. Z pewnością wskazane jest również zawarcie porozumień pomiędzy centrami zarówno krajowymi, jak i międzynarodowymi. Taka współpraca, szczególnie z bardziej już dojrzałymi organizacjami zagranicznymi, pozwoli na szybsze reagowanie w celu powstrzymania ataku, a wręcz zapobiegania jego wystąpieniu.

Bibliografia

Pawlik M., *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych*, „Problemy Kolejnictwa" 2021, z. 191.

Pawlik M., *Wytyczne dotyczące cyberbezpieczeństwa dla pracowników podmiotów kolejowych* [w:] *Magazyn kultury bezpieczeństwa*, Warszawa 2021.

Railway Cybersecurity. Good practices in cyber risk management, European Union Agency for Cybersecurity ENISA, November 2021, https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management [dostęp: 25.01.2023].

Railway Cybersecurity, security measures in the Railway Transport Sector, European Union Agency for Cybersecurity ENISA, November 2020, https://cyberpolicy.nask.pl/wp-content/uploads/2021/01/ENISA-Report-Railway-Cybersecurity.pdf [dostep: 25.01.2023].

Standardy techniczne. Szczegółowe warunki techniczne dla budowy infrastruktury kolejowej Centralnego Portu Komunikacyjnego – wytyczne projektowania, t. 18, *Wymagania w zakresie spójności bezpieczeństwa, ochrony i cyberbezpieczeństwa*, wersja 1.3.0, Warszawa 2021.

Transport cybersecurity toolkit, European Union 2020, https://www.fecc.org/wp-content/uploads/2020/12/DG-MOVE-Transport-Cybersecurity-Toolkit-FINAL.pdf [dostęp: 5.12.2022].

Zoning and conduits for railways, European Union Agency for Cybersecurity ENISA and European Rail ISAC, February 2022, https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways [dostęp: 25.01.2023].

The role of the Information Sharing and Analysis Centers' n building the resilience of the key sectors of the Polish economy

Abstract

As the threats from cyberspace to IT systems (information technology) and digital OT systems (operational technologies) using ICT technologies (information and communication technologies) grow exponentially, while at the same time the scale of the use of digital data collecting, processing and sharing for the needs of many national economy areas and to support functioning of the state in terms of, for example, defence, health care, education or citizen services, building awareness of the risks and skills to secure networks, systems and digital services against cyber threats becomes crucial. A new type of structures called ISACs (Information Sharing and Analysis Centres) play an important role in this respect. The co-authors, based on the provisions of the law and their own experience in ISAC-Kolej and ISAC-GIG centers, present the ecosystem around ISAC centers, their tasks and challenges.

Key words: cybersecurity, key service operators, ISACs Information Sharing and Analysis Centers

Andrzej Pieczywok*

Cyberspace as a source of dehumanization of the human being

Abstract

The paper points to an important sphere of human safety, as it refers to cyberspace as an environment where information is exchanged via the net and computer systems. In addition to positive accents, cyberspace also creates various threats that lead to the dehumanization of life. The negative effects of being in cyberspace cause threats to mental, social and healthy lives. Very often they pose a danger not only to human health but also to human life. In addition to the introduction, the article includes characteristics of the loss of a sense of reality among people who use cyberspace excessively and the risks of medical hazards.

Key words: cyberspace, cybersecurity, institutional threats, personal threats, risk

* Assoc. Prof. Andrzej Pieczywok, PhD, Kazimierz Wielki University in Bydgoszcz, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

Introduction

The terms „safety"[1] and „cyber harassment"[2] are categorised as terms of great significance in the sphere of human functioning and frequently appear both in theoretical considerations and in everyday speech.

We live in a unique time in human history, an intense period of change and disruption related to human existence. It seems to us that the reality we live in has always existed this way, but never before have we lived in a world so subservient to our needs. The mass media play a key role in people's lives. Their importance is evident in the amount of time people spend watching TV, surfing the World Wide Web, listening to music or reading newspapers and magazines. The delivery of information through mass media is immediate and available around the clock. As part of media coverage we need to start thinking and talking more and more often about the negative impacts of the cyberspace technological environment on both the individual and society. Virtual spaces now allow us to satisfy our senses with visions we cannot resist.

Modern man, thanks to developments of technology, increasingly escapes into the virtual world simulating reality, enriching the form of experiences of the present world and desires for an easy future. Cyberspace is a constantly evolving and expanding environment that is being used for an increasing number of purposes. Cyberspace is a growing aspect in almost all areas of human life and needs. On the one hand, it helps promote people's welfare, educates society and improves the quality of life. On the other hand, cyberspace inflames ethnic and religious tensions, sows discord and causes suffering. The ease of access to cyberspace and the range of hacking tools available, in combination with the inherent insecurity of the Internet, mean many different threats.

1 See: A. Pieczywok, *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018, p. 13; M. Czuryk, K. Drabik, A. Pieczywok, *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018, p. 7; J. Gierszewski, A. Pieczywok, *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018; M. Karpiuk, *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, no. 9, p. 10–17; A. Pieczywok, *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021, p. 20–21.

2 See: M. Górka, *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017, p. 20; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2, p. 62.

Cyberspace is a dynamic and complex environment, making the prospect of securing it a difficult undertaking. It is said that „If you cannot measure it, you cannot improve it" and this can be applied to cybersecurity[3]. It seems that visual art may become more important today than at any time in the past.

Gradually, the term „cyberspace" has come to be used by scientists to identify phenomena that are not the product of human imagination, to name links of a virtual nature[4].

Some authors define cyberspace as a network of IT infrastructure interdependencies that consist of the Internet, telecommunications networks, computer systems, embedded processors and controllers in the industrial environment of strategic importance[5], as well as copper cables, Internet routers, optical fibres, relay towers and satellite transponders[6].

Pierre Lévy, a French sociologist and author of the term „cyberculture" defines cyberspace as „a new space of communication, sociability, organization and transaction"[7]. The sociologist also points to the emergence of a new market for information and knowledge as a result of modern technological evolution. Cyberspace is a subject of study for sociologists, and references to the achievements of this scientific discipline are found in some state cybersecurity strategies.

A person using cyberspace is both its creator (designer) and consumer and uses other people's output in both permitted and unauthorised ways. Humans co-create cyberspace through graphics, selfies, opinions, photos, comments, recordings, likes, downloads, biometrics, views, purchases, locations, etc. This phenomenon seems to be the beginning of a process of significant growth in the initiative and creativity of the individual, as virtual space offers more and more opportunities for artistic expression in front of a myriad audience – co-participants of this process. This impact of cyberspace on modern man is becoming increasingly apparent and worrisome.

The purpose of the article is to highlight the negative issues of being in cyberspace, especially its impact on the dehumanization of human life.

3 S. Katzman, *Operational Assessment of IT*, Boca Raton, FL 2016, p. 23.

4 R. Aleksandrowicz, K. Liedel, *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [in:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, ed. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014, p. 23.

5 H. Katzan, *Cybersecurity Service Model*, „Journal of Service Science" 2012, vol. 5, no. 2, p. 72.

6 M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, p. 82.

7 P. Levy, *Drugi potop*, http://portal.tezeusz.pl/cms/tz/index.php?id=287 [access: 20.02.2022].

Manifestations of the loss of a sense of reality

The development of the Internet from one day to the next, covering all aspects of life, puts humans between two worlds: the real and the virtual one. The dominance of virtual environments in all aspects of human personality, especially identity, is evident. The emergence of virtual identities in cyberspace, besides real ones, is one of the challenges of the virtual environment of the Internet.

Unfortunately, at a time when cyberspace is becoming a virtual reflection of physical reality, negative forms of human activity are also infiltrating it. Constructed for scientific cooperation, the Internet network provides a great sense of anonymity and is used by criminals, terrorists, as well as some states, to carry out illegal activities or aggression against other entities.

In the study of cyberspace and virtual reality, it is common in the above cases to talk about alternate, side lives. Digital fiction replaces reality for humans and is so much more attractive because anything is possible in it. Leaving such a developed and idealised digital space causes painful feelings. Returning to the real world – inferior, less interesting, limited by many laws, rules and conditions – causes a person to feel psychological discomfort, or even observe in himself syndromes of serious addiction[8].

People behave differently when they interact with technology, compared to face-to-face interactions with the real world: Whenever technology combines with basic human tendencies, the result is empowerment and acceleration.

Describing cyberspace as a source of dehumanization of human beings, it is worth noting some manifestations of the loss of a sense of reality. Evidence points to the occurrence of significant harm to both individuals and society. Some of these harmful effects include information overload (information overload is associated with a loss of control, feeling overwhelmed, reduced intellectual performance and reduced job satisfaction); damage to social relationships (loneliness and social isolation); violation of public/private boundaries (the blurring of distinctions between different spheres of life, including work, home life and leisure); detrimental effects on cognitive development (development of memory skills, attention, critical reasoning skills, language acquisition, reading and learning abilities); damage to communities (partial migration of human activities to the Internet – shopping, commerce, socialising, recreational activities, professional interactions).

8 Cf. A. Jaszczak, *Poczucie uzależnienia od Internetu a poczucie kontroli u adolescentów* [in:] *Psychologiczne konteksty Internetu*, ed. B. Szmigielska, Kraków 2009, p. 238.

Many researchers point to the danger of a detached sense of reality among the youngest users of cyberspace. They include cognitive dysfunctions which may lead to an inability to continue learning, perceptual disturbances, fluency of attention, reduced ability or a loss in the ability to think logically, sense of confusion, intrusive thoughts, compulsive behaviour, and memory disorders. In addition, there is psychological discomfort that occurs as a result of drastic interventions, the so-called withdrawal syndrome, which sometimes has a drastic course[9].

Humans do not so much participate in the world constructed by cyberspace, but most of all this world becomes part of their nature. From the point of view of epistemology, this paradox of "immersion" is among the most interesting aspects of the new reality[10]. It means, first of all, the possibility of participation in the supra-individual impersonal total, transcending the physical boundaries of time and space[11]. In a space described in this way, the boundaries of human subjectivity and identity, which are the foundations of human rationality, are blurred, and therefore the sense of reality is at risk.

This virtual presence is a step towards alienation, dehumanization, and the loss of a sense of ethics and axiology. According to Richard Spinello „It would be most appropriate to adopt the position that moral values must be the ultimate regulator of cyberspace"[12].

Andrzej Kiepas notes that, in a virtual space, humans change their valuation: „A man deprived of value is a man not only deprived of identity but also deprived of the conditions for building it. […] Entering the virtual world must therefore involve the need to take accountability, which is particularly difficult in the situation of web dependencies and the axiological opacity of the world we face. Immersed in the world of momentary structures, humans may have certain difficulties in this regard"[13].

9 Cf. M. Jędrzejko, *Narkotyki w Internecie – nowe zjawisko, nowy problem społeczny i wychowawczy* [in:] *Oblicza Internetu. Opus Universale. Kulturowe, edukacyjne i technologiczne przestrzenie Internetu*, ed. M. Sokołowski, Elbląg 2008, p. 184.

10 Cf. D. de Kerckhove, *Die Architektur der Intelligenz. Wie die Vernetzung der Welt unsere Wahrnehmung verändert*, Basel 2002, p. 48.

11 Cf. Z. Suszczyński, *Hipertekst a „galaktyka Gutenberga"* [in:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, ed. M. Hopfinger, Warszawa 2005, p. 531.

12 R. Spinello, *CyberEthics, Morality and Law in Cyberspace*, New York 2000, p. 45.

13 A. Kiepas, *Podmiotowość człowieka w perspektywie rozwoju rzeczywistości wirtualnej* [in:] *Media i edukacja w globalizującym się świecie. Teoria, praktyka, oddziaływanie*, ed. M. Sokołowski, Olsztyn 2003, p. 417.

Medical hazards

Health is also a value that can be felt (perceived as valuable) and/or recognised (related to the belief that health should be valued) by the individual. It can be a ceremonial value (belonging to higher, universally respected values) or an everyday value (important for the fulfilment of the individual's private objectives). Finally, health is classified as a declared or realised value[14].

Prolonged work in cyberspace (computer addiction) can cause physical damage. Using a mouse and keyboard for many hours every day can lead to repetitive strain injuries. Back problems are common among people who spend a lot of time sitting at desks. Computer addiction can indirectly lead to a poor overall physical condition and even obesity. The improper placement of computer equipment can strain the shoulders. Too much of this activity stretches the shoulder muscles, resulting in cramps, fatigue, headaches and stiffness in the neck and shoulders. Long-term sleep deprivation causes lethargy, difficulty concentrating and depression of the immune system.

Some health problems caused by active participation in cyberspace include: 1) musculoskeletal problems – neck and back pain, as well as pain in the elbows, wrists and hands. In addition to back pain caused by computer use, often resulting from poor gaming posture or computer posture, there have also been reports of „selfie elbow" or „texting thumb" caused by the overuse of technology; 2) digital eye fatigue – symptoms of digital eye fatigue include dry eyes, redness around the eyes, headaches, blurred vision and neck and shoulder pain; 3) disrupted sleep – symptoms of disrupting the biological clock, activities on digital devices can stimulate and significantly reduce sleep readiness; 4) physical inactivity – too much of a sedentary lifestyle is associated with an increased risk of several conditions including obesity, heart disease, cancer and diabetes; 5) psychological issues – excessive time spent in front of a screen can negatively affect mental and emotional wellbeing. Social media users who log in several times a day may be exposed to non-stop news, usually bad news, such as natural disasters, terrorist events, political divisions, high-profile crimes, etc.; 6) the negative impact on children – children's brains may be more vulnerable to the effects of technology overuse, this affects social skills, creativity, attention span and delays in language and emotional development;

14 B. Woynarowska, *Zdrowie – podstawowe pojęcie w edukacji zdrowotnej* [in:] *Edukacja zdrowotna*, ed. eadem, Warszawa 2017, p. 15.

7) an impact on hearing – is at risk due to unsafe listening practices, partly due to listening to music through headphones or earbuds.

It is worth mentioning that health problems occasioned by the active participation of man in cyberspace cause a variety of ailments, and paying attention to back pain it can be said that it is one of the most common causes of disability among active people. The spine is responsible for correct posture and also for most movement. Cervical spine pain is in second place in terms of the number of spine-related complaints. People with sedentary lifestyles, and especially those who work in a sitting position (computer work), more and more often complain about it. Spinal pain may be accompanied by a feeling of tingling or numbness in one of the limbs. Also, spinal pain is accompanied by a feeling of weakness in the legs.

To meet the problems of the dangers posed by cyberspace, it is worth taking preventive measures to make children, adolescents and adults aware that the development and use of modern technology pose dangers that can affect everyone.

In conclusion, it should be said that cyberspace as a source of dehumanization particularly jeopardizes human health, and has quite an impact on the manifestation of the loss of a sense of reality. Long hours spent at a computer or with a smartphone in hand, without a dose of exercise will turn man from *homo sapiens* to *homo computerus*. Apparently, the most effective way to reduce cybersecurity threats is to periodically implement training and education for young people in schools. Security education should be a continuous process, aimed at the most comprehensive development of skills and personality, as well as general mental fitness.

Simple rules that every computer user should follow are significant, too. It is very important to put less strain on your shoulders, so place the keyboard and mouse where you do not have to strain to reach them. The mouse should be comfortably close, the table should be at a height where you do not have to reach up while typing on the keyboard. Good writing techniques should be practised to avoid hand problems. When working at a computer, take a 10-minute break every hour. The monitor should be directly in front of the user at a distance of 24–26 inches from the user. You should also use larger fonts and good colour contrast, which will reduce eye fatigue while working.

Bibliography

Aleksandrowicz R., Liedel K., *Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia* [in:] *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, ed. K. Liedel, P. Piasecka, T.R. Aleksandrowicz, Warszawa 2014.

Czuryk M., Drabik K., Pieczywok A., *Bezpieczeństwo człowieka w procesie zmian społecznych, kulturowych i edukacyjnych*, Olsztyn 2018.

Gierszewski J., Pieczywok A., *Społeczny wymiar bezpieczeństwa człowieka*, Warszawa 2018.

Górka M., *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Warszawa 2017.

Jaszczak A., *Poczucie uzależnienia od Internetu a poczucie kontroli u adolescentów* [in:] *Psychologiczne konteksty Internetu*, ed. B. Szmigielska, Kraków 2009.

Jędrzejko M., *Narkotyki w Internecie – nowe zjawisko, nowy problem społeczny i wychowawczy* [in:] *Oblicza Internetu. Opus Universale. Kulturowe, edukacyjne i technologiczne przestrzenie Internetu*, ed. M. Sokołowski, Elbląg 2008.

Karpiuk M., *Ograniczenie wolności uzewnętrzniania wyznania ze względu na bezpieczeństwo państwa i porządek publiczny*, „Przegląd Prawa Wyznaniowego" 2017, no. 9.

Katzan H., *Cybersecurity Service Model*, „Journal of Service Science" 2012, vol. 5, no. 2.

Katzman S., *Operational Assessment of IT*, Boca Raton, FL 2016.

Kerckhove de D., *Die Architektur der Intelligenz. Wie die Vernetzung der Welt unsere Wahrnehmung verändert*, Basel 2002.

Kiepas A., *Podmiotowość człowieka w perspektywie rozwoju rzeczywistości wirtualnej* [in:] *Media i edukacja w globalizującym się świecie. Teoria, praktyka, oddziaływanie*, ed. M. Sokołowski, Olsztyn 2003.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015.

Levy P., *Drugi potop*, http://portal.tezeusz.pl/cms/tz/index.php?id=287 [access: 20.02.2022].

Pieczywok A., *Działania społeczne w sferze bezpieczeństwa wewnętrznego*, Lublin 2018.

Pieczywok A., *Idee bezpieczeństwa człowieka w teoriach i badaniach naukowych*, Bydgoszcz 2021.

Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2.

Spinello R., *CyberEthics, Morality and Law in Cyberspace*, New York 2000.

Suszczyński Z., *Hipertekst a „galaktyka Gutenberga"* [in:] *Nowe media w komunikacji społecznej w XX wieku. Antologia*, ed. M. Hopfinger, Warszawa 2005.

Woynarowska B., *Zdrowie – podstawowe pojęcie w edukacji zdrowotnej* [in:] *Edukacja zdrowotna*, ed. B. Woynarowska, Warszawa 2017.

Cyberprzestrzeń jako źródło dehumanizacji człowieka

Streszczenie

Treść artykułu wskazuje na istotny obszar bezpieczeństwa człowieka, dotyczy bowiem cyberprzestrzeni jako środowiska wymiany informacji za pomocą sieci i systemów komputerowych. Cyberprzestrzeń oprócz pozytywnych akcentów powoduje też powstawanie różnych zagrożeń, które prowadzą do dehumanizacji życia człowieka. Negatywne skutki bycia w cyberprzestrzeni powodują zagrożenia dotyczące życia psychicznego, społecznego i zdrowotnego. Bardzo często zagrażają nie tylko zdrowiu człowieka, lecz także i jego życiu. Artykuł oprócz wprowadzenia zawiera charakterystykę utraty poczucia rzeczywistości wśród osób nadmiernie korzystających z cyberprzestrzeni oraz ryzyko zagrożeń zdrowotnych.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, zagrożenia instytucjonalne, zagrożenia osobowe, ryzyko

Mirosław Karpiuk*

The executive agency as a legal organisational form of implementing cybersecurity tasks

Abstract

The national cybersecurity system is formed of a number of public entities, including executive agencies with legal personality as entities of the public finance sector. The executive agency could implement cybersecurity tasks important to the functioning of the state and its institutions. Through this legal organisational form, it would be possible to shape the development of new technologies that could then serve a digital society or digital state, including the protection of ICT systems for communication, as well as the provision of digital services and key services. Due to the widespread activity in cyberspace, it is necessary to have entities in place to protect its users. Such an entity could have the form of a cyber agency, working with other institutions (public and private), that is competent for cybersecurity.

Key words: cybersecurity, cyberspace, executive agency

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

Introduction

There is a clear realisation that the development of new technologies, both civilian and military ones, contributes to a significant increase in the employment of unmanned and autonomous systems, automated and robotised weapon platforms using artificial intelligence, as well as long-range precision weapon systems. Digital technologies are advancing rapidly, and the development of solutions based on fixed line and mobile broadband, the Internet of Things, cloud computing, quantum technologies, automation of services, nanotechnology and artificial intelligence creates new development opportunities for Poland, while also generating previously unknown threats. The challenge for the state consists in joining the technological race in this area, which would offer Poland the opportunity to overcome the position of a mere user and join a group of countries with effectively functioning digital economies, providing solutions and co-creating international standards. It should be stated that communication systems are a key component of national security assets and preparatory measures for crisis situations, so they constitute an important element of the national critical infrastructure. In this respect, a key challenge is to develop secure and modern telecommunications networks capable of handling the increasing number of end users and systems. In the context of the digital revolution, the specific roles of cyberspace and information space should be taken into account. This also creates room for disinformation and the manipulation of information, which requires effective strategic communication activities[1].

Social and economic development is more and more dependent on fast and unhindered access to information and its use in management, production, services and the public sector. The dynamic progress of information systems serves the national economy. The use of digital technologies that comprise cyberspace affects the formation of social relationships, and online services have become a tool for influencing the behaviour of social groups, as well as a means of exerting political influence[2].

Ensuring digital security is one of the primary tasks of state authorities. Threats of an IT nature have increasingly serious consequences, and

1 *National Security Strategy of the Republic of Poland*, Warszawa 2020, p. 7–8.

2 Cybersecurity Strategy of the Republic of Poland – Annex to Resolution no. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazette of the Republic of Poland 2019, item 1037).

cyberattacks can be used as a means of economic as well as political pressure[3]. The executive cyber agency could play its part in ensuring digital security, which may additionally support the development of new technologies that could also be used to ensure this security.

Cybersecurity, defined as the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[4], could also be the spectrum of an executive agency set up for this purpose, especially in an era where cyberattacks are not only more and more frequent, but also carry more and more consequences. Since information systems are now the basis of many areas of public, private, or social activity, or are an instrument supporting or greatly facilitating such activity, they must not only develop rapidly, but must also be properly protected. Such tasks can be given to the cyber agency.

The place of the cyber agency in the national cybersecurity system

Pursuant to Art. 3 of the NCSA, the objective of the national cybersecurity system is to ensure cybersecurity at the national level, including the uninterrupted provision of essential services and digital services by achieving an appropriate level of security for the information systems used to provide these services, and ensuring the handling of incidents[5]. The executive agency,

3 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 145.

4 Art. 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2020, item 1369, as amended) – hereinafter referred to as the NCSA For more information about cybersecurity refer to: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *Activities of the local government units in the field of telecommunications*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2.

5 See also: I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1, p. 175.

as an entity of the public finance sector, will also be among the entities included in the national cybersecurity system, as provided for by Art. 4(7) of the NCSA. It will therefore be obliged to ensure that information systems are protected in such a way as to allow the uninterrupted provision of essential services and digital services.

The executive agency is therefore a public-finance sector entity. At the same time, it should be emphasised that separating the public finance sector makes it easier to draw the circle of entities obliged to apply certain universal principles of financial management specific to public sector entities[6].

Legal organisational form

The executive agency can serve as one of the legal organisational forms through which to perform cybersecurity tasks. This form has already become a permanent fixture in the Polish political and legal space. Not only is it recognisable, but its mechanisms are already proven on many levels of operation, so there is a high probability that in the realm of cybersecurity it can properly fulfil the tasks assigned to it.

Cybersecurity matters in the military dimension fall within the competency of the Minister of National Defence, while cybersecurity in the civilian dimension is the responsibility of the minister competent for computerisation[7]. Depending on the status of such an agency, one of these ministers would supervise its activities.

Executive agencies are regarded as the new management governance instrument, which is defined as the orientation of public administration to achieve specific results through the implementation of specific tasks, which should be verified on the basis of measurable standards or indicators. In this perspective, the public administration becomes responsible for the efficient provision of services[8]. The executive agency could therefore work effectively in cyberspace, in terms of both developing new cyber technologies and

6 M. Cilak [in:] *Ustawa o finansach publicznych. Komentarz*, ed. Z. Ofiarski, Warszawa 2020, art. 9.

7 Art. 12a and 19 of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended). See also M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1, p. 86–87.

8 K. Marchewka-Bartkowiak, *Agencje wykonawcze*, „Infos" 2011, no. 19, p. 1.

countering cyber threats. Innovation is the spectrum of activities that the executive agency can successfully deal with. Its rules would have to be detailed in the statute.

The executive agency is a state-owned legal entity formed under statutory law to carry out the state's tasks[9]. The solutions adopted for executive agencies by the Polish legislator were modelled on EU legislation[10].

Organisational structure

The organisational structure of the cyber agency can be mapped to already existing executive agencies dealing with other issues. Certain legal solutions for the organisational structure could be borrowed from the statutory solutions adopted, for example, from the Military Property Agency[11], applying them to the cyber agency, accordingly, while taking into account the specifics of its activities.

Thus, the cyber agency would be an executive agency within the meaning of the APF, supervised by the Minister of National Defence or the minister competent for computerisation (depending on the scope of its activities – cybersecurity in the military dimension or cybersecurity in the civilian dimension). It would operate on the basis of statutory law and the statute. It would consist of: 1) the Office of the Head of the Cyber Agency; 2) regional branches (if formed). The Minister of National Defence or alternatively, the minister competent for computerisation (competent minister), by way of regulation, would determine the statute of the cyber agency, specifying its internal organisation, including a list of managerial positions in the Office of the Head of the Cyber Agency, as well as a list of regional branches, and their the substantive and local jurisdiction, taking into account the need to ensure the efficient performance of the agency's tasks. The cyber agency bodies could be: 1) the Head of the Cyber Agency; 2) the Supervisory Board; 3) directors of regional branches (if formed).

9 Art. 18 of the Act of 27 August 2009 on Public Finance (consolidated text, Journal of Laws 2021, item 305, as amended), hereinafter the APF.

10 See Council Regulation (EC) no. 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes (Official Journal of the European Union 2003, L 11, p. 1).

11 The Act of 10 July 2015 on the Military Property Agency (consolidated text, Journal of Laws 2021, item 303, as amended).

The Head of the Cyber Agency would be appointed and dismissed by the President of the Council of Ministers on the proposal of the competent minister. Appointment to the role would mean the establishment of an employment relationship. The term of office would last three years. The term of office of the Head of the Cyber Agency would expire upon: 1) his death; 2) resignation; 3) dismissal. After the expiration of the term of office of the Head of the Cyber Agency for the reasons specified above, his duties would be performed by his deputy designated by the competent minister, until the new Head of the Cyber Agency assumes his duties. The position of the Head of the Cyber Agency could be held by a person who: 1) has a master's degree or equivalent; 2) is a Polish citizen; 3) enjoys full public rights; 4) has not been validly sentenced for an intentional crime or an intentional fiscal crime; 5) has managerial competence; 6) has at least six years of work experience, including at least three years of work experience in a managerial position; 7) has education and knowledge related to matters falling within the competency of such an agency.

The Head of the Cyber Agency would act with the assistance of not more than four deputies and directors of regional branches (if formed). Deputies of the Head of the Cyber Agency would be appointed and dismissed by the competent minister upon the proposal of the Head of the Cyber Agency. Executive positions in the Office of the Head of the Cyber Agency would be appointed and dismissed by the Head of the Cyber Agency. These appointments would imply the establishment of an employment relationship within the meaning of the Labour Code.

The cyber agency's regional branches would be formed for the area of one or more provinces or parts thereof. Regional branches would be managed by directors with the help of deputies. The cyber agency's regional branch directors and their deputies would be appointed and dismissed by the Head of the Cyber Agency. Appointment to these roles would mean the establishment of an employment relationship.

In civil cases the cyber agency would be represented before courts by the Head of the Cyber Agency and by regional branch directors having the substantive and local jurisdiction. In labour law cases the cyber agency would be represented before courts by the Head of the Cyber Agency with respect to employees working in the Office of the Head of the Cyber Agency and by competent directors of the regional branches, having substantive and local jurisdiction, with respect to employees working in the regional branches.

The Supervisory Board would consist of seven members appointed by the relevant minister in consultation with the minister competent for public

finance. The relevant minister, in consultation with the minister competent for public finance, could dismiss the Supervisory Board or its individual members during the term of office. In the case of dismissal of a member of the Supervisory Board, a new member would be appointed for the remainder of the ongoing term of office of the Supervisory Board. The Supervisory Board would be composed of five representatives of the relevanrt minister and two representatives of the minister competent for public finance. The chairman of the Supervisory Board would be appointed for the term of office by the relevant minister from among the members of the Supervisory Board. The relevant minister could dismiss the Chairman of the Supervisory Board during his term of office at any time. Removal from this office would not mean removal from the Supervisory Board. The term of office of the Supervisory Board would be three years. The term of office of a member of the Supervisory Board would expire upon: 1) his death; 2) resignation; 3) dismissal. The Supervisory Board would exercise permanent supervision over the cyber agency's activities.

Financial economy

The basis of the executive agency's financial economy (as is clear from Art. 21 of the APF) is an annual financial plan comprising of: 1) revenue; 2) subsidies from the state budget; 3) a statement of the operational costs of the executive agency, as well as the costs of performing statutory tasks, distinguishing the costs of having other entities perform these tasks – specifying salaries and contributions calculated on them, payments of interest arising from incurred liabilities and the purchase of goods and services; 4) the financial result; 5) funds for capital expenditures; 6) funds allocated to other entities; 7) the balance of receivables and liabilities at the beginning and end of the year; 8) the balance of cash at the beginning and end of the year. The annual financial plan of the executive agency is drafted by its competent authority in consultation with the minister exercising supervision over the executive agency. After approval by the minister exercising supervision, the draft is forwarded to the Minister of Finance. Within the framework of the draft financial plan, a plan of revenue and expenditures of the executive agency recognised on the date of their payment is drawn up, and in this plan of revenue and expenditures, the planned expenditures should not be higher than the planned revenues. Planned expenditures may exceed planned revenue in exceptional instances, but only with the approval of the minister supervising

the executive agency, issued in consultation with the Minister of Finance. The financial plan of the executive agency may be amended in terms of revenue and expenses after obtaining the approval of the minister exercising supervision over the agency, which is issued after obtaining the opinion of the parliamentary committee responsible for the budget. The Minister of Finance must be notified immediately of any amendments made. As a rule, amendments to the executive agency's financial plan may not result in an increase in the agency's liabilities or worsen the agency's projected financial result. The executive agency may receive subsidies from the state budget, to the extent specified in statutory law under which it is formed. It may incur obligations for the period of performance of a given task exceeding the budgetary year, if the expenses necessary to service the debt are recognised in the annual financial plan.

Financial plans of executive agencies are also included in annexes to the state budget act as required under Art. 122(1)(1)(a) of the APF The financial plans of executive agencies, annexed to the state budget act, are of special character, thus due to their nature and subject matter they cannot be directly included in the state budget. They cannot be mechanically or accountably attached to the state budget, they must function separately[12].

The statutorily guaranteed minimum level of detail of the executive agency's financial plan is a manifestation of openness in the management of public funds. The regulations also provide for a special procedure for determining the executive agency's financial plan, which involves cooperation and supervision by various bodies. It consists in delegating authority in this regard to the competent authority, acting in consultation with the minister exercising supervision over the executive agency. The draft version of the financial plan is subject to approval by the minister exercising supervision[13].

The executive agency's financial economy rules are quite rigid in nature. It is not permitted, without an amendment to the state budget act in the part being an annex containing the financial plan of a given executive agency, to change its financial plan, which consists in a simultaneous increase in its own revenues and costs of performing its tasks, since the above amounts are presented in the state budget act[14].

However, the disadvantage of such an agency is the obligation to pay surplus funds into the state budget. Such rules for the settlement of surplus

12 A. Borodo [in:] *Ustawa o finansach*..., art. 122.
13 L. Lipiec-Warzecha, *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011, art. 21.
14 K. Kopyściańska [in:] *Ustawa o finansach*..., art. 21.

funds are laid down in Art. 22 of the APF Thus, the executive agency is obliged to pay annually to the state budget, to the account of the revenues of the state budgetary unit serving the minister supervising the agency, the surplus of the funds, determined at the end of the year, which remains after settling tax liabilities. This surplus shall be transferred by the executive agency as soon as the liabilities due from the reporting period are settled, but no later than on 30 June of the year following the year in which the surplus arose. In particular, justified cases arising from the need to ensure the efficient and full performance of the tasks of the executive agency, the Council of Ministers may, at the request of the minister exercising supervision over the executive agency, agree, by resolution, not to pay surplus funds into the state budget. The Minister exercising supervision over the executive agency, in consultation with the Minister of Finance, shall decide, by way of regulation, the method of determining the surplus, having regard for the need to ensure continuity of funding for the Agency's tasks, making investments necessary for the performance of state tasks, and taking into account the funding sources for the tasks carried out by the agency. Such regulation would also have to be issued with respect to the executive cyber agency.

Therefore, the regulation should specify how to determine the surplus of the cyber agency's funds that are subject to payment into the state budget. The surplus of the agency's funds shall be determined by taking into account the income received from sources other than the state budget and the expenses incurred by the cyber agency, with the exception of expenses for the performance of the tasks for which the agency received funds from the state budget. Furthermore, the surplus of the agency's funds shall be determined by taking into account the funds deposited in bank accounts at the end of the budgetary year, except for: 1) dividends; 2) unused funds from reimbursable grants, funds from the budget of the European Union and non-reimbursable funds from aid provided by member states of the European Free Trade Agreement (EFTA); 3) restricted funds: (a) of the employee benefit fund and the repair & renovation fund, (b) bid securities, (c) guarantee deposits and performance bonds, (d) prepayments made by the agency's contractors deposited in the agency's bank accounts at the end of a given budgetary year, including prepayments made to the agency as part of the implementation of tasks in the area of national defence and state security, (e) overpayments and erroneous payments made by the agency's contractors, (f) funds deposited in the VAT account. When determining the surplus of funds, the funds to be settled shall be reduced by the tax liabilities determined at the end of the budgetary

year, or liabilities due by 31 March of the following year, excluding liabilities related to funds not taken into account when determining the surplus[15].

All executive agencies are required to pay annually to the state budget any surplus funds obtained as a result of their activities, and payments of these surplus funds should be classified as a type of untaxed revenue of the state budget[16]. Executive agencies, being unable to keep surplus funds for themselves, should not thereby be incentivised to achieve a surplus[17].

The cyber agency should receive an operating subsidy from the portion of the state budget administered by the Minister of National Defence if the funds planned to be earned from operations would not be sufficient enough to cover operational costs. It should also receive an earmarked subsidy from the portion of the state budget administered by the Minister of National Defence for carrying out certain assigned tasks.

Financial support for cyber agencies could also be provided through the Cyber Security Fund. Its statutory objective is to support efforts to ensure that communication and information systems are guaranteed protection against cyber threats. This is an earmarked state fund, the administrator of which, in the current state of law, is the minister competent for computerisation[18]. Since the Cyber Security Fund currently makes payments of telecommunications benefits, subsidising other areas of activity would require an amendment to statutory law.

Attention should be paid to the transparency and integrity of the executive agency's management, especially in terms of financial management, which determines the need to implement internal control procedures, as well as to define a clear mechanism for external control of its activities.

15 Cf. § 1–3 of the Regulation of the Minister of National Defence dated 24 October 2017 on Determining Surplus Funds of the Military Property Agency (consolidated text, Journal of Laws 2019, item 2299).

16 K. Kopyściańska [in:] *Ustawa o finansach*…, art. 22.

17 C. Kosikowski, *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011, art. 22.

18 Art. 2 of the Act of 2 December 2021 on Special Rules of Remuneration for Persons Performing Cybersecurity Tasks (Journal of Laws 2021, item 2333, as amended). See also M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Conclusions

The legal organisational form of the executive agency can be used to perform public tasks that are important for the functioning of the state, including its (cyber) security. Based on the example of EU solutions, as well as those adopted in Poland, it can be seen that executive agencies perform tasks mostly in areas such as research and development, or new technologies, and therefore could (effectively, it seems) perform the tasks arising from the sphere of cybersecurity. The cyber agency could be a non-commercial business-support institution, which can positively influence not only the development of the business environment, but also the development of the region in which such an agency is based or operates. It could also establish cooperation with various entities from both the public and private sectors, as well as the social sector, depending on the projects being implemented.

The cyber agency's objectives must correspond to the strategic objectives defined in both the Security Strategy of the Republic of Poland and the Cybersecurity Strategy of the Republic of Poland. These include: 1) enhancing resilience to cyber threats and increasing the level of protection of information in both the civilian and military sectors, as well as promoting knowledge and good practices to better protect information; 2) developing the national cybersecurity system using private and public capabilities; 3) enhancing resilience of information systems and achieving the ability to effectively prevent and respond to incidents; 4) enhancing national cybersecurity capabilities; 5) building public awareness and competence in the field of cybersecurity; 6) building a strong international position of the Republic of Poland in the area of cybersecurity; 7) enhancing the resilience of information systems used in the military sphere and achieving the ability to effectively prevent, combat, and respond to cyber threats; 8) strengthening the defensive capabilities of the state by ensuring the continued development of the national cybersecurity system; 9) achieving the ability to conduct a wide range of military and non-military activities in cyberspace; 10) developing national capabilities in the area of testing, research and the evaluation of cybersecurity solutions and services; 11) developing competence, knowledge and the awareness of threats and challenges among public administration personnel and society in the area of cybersecurity; 12) strengthening and expanding the capabilities of the state through the development of indigenous solutions in the area of cybersecurity and conducting state-funded research and development in the area of modern technologies, among others; 13) establishing cooperation,

including universities and scientific institutions and companies, both in the public and private sector; 14) enhancing the cybersecurity of essential and digital services, as well as of critical infrastructure; 15) expanding industrial and technological resources for the purposes of cybersecurity in the military dimension[19].

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.
Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.
Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.
Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2
Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2.
Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.
Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.
Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Kosikowski C., *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011.
Lipiec-Warzecha L., *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011.
Marchewka-Bartkowiak K., *Agencje wykonawcze*, „Infos" 2011, no. 19.
National Security Strategy of the Republic of Poland, Warszawa 2020.
Ustawa o finansach publicznych. Komentarz, ed. Z. Ofiarski, Warszawa 2020.

19 See also M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, ibidem 2021, no. 1, p. 47–50.

Agencja wykonawcza jako forma organizacyjno-prawna realizacji zadań ze sfery cyberbezpieczeństwa

Streszczenie

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów publicznych, w tym posiadające osobowość prawną agencje wykonawcze będące jednostkami sektora finansów publicznych. Agencja wykonawcza mogłaby również realizować zadania z dziedziny cyberbezpieczeństwa, jako ważne z punktu widzenia funkcjonowania państwa i jego instytucji. Za pośrednictwem tej formy organizacyjno-prawnej można byłoby kształtować rozwój nowych technologii, które mogłyby następnie służyć cyfrowemu społeczeństwu czy też cyfrowemu państwu, w tym chronić systemy teleinformatyczne służące komunikowaniu się, a także świadczeniu usług cyfrowych i usług kluczowych. Ze względu na powszechną aktywność w cyberprzestrzeni muszą istnieć podmioty, które będą chronić jej użytkowników. Takim podmiotem może być cyberagencja współpracująca z innymi instytucjami (publicznymi i prywatnymi), właściwa w sprawach cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, agencja wykonawcza

Michał Zimoń*
Rafał Kasprzyk**

Yet another research on GANs in cybersecurity

Abstract

Deep learning algorithms have achieved remarkable results in a wide range of tasks, including image classification, language translation, speech recognition, and cybersecurity. These algorithms can learn complex patterns and relationships from large amounts of data, making them highly effective for many applications. However, it is important to recognize that models built using deep learning are not fool proof and can be fooled by carefully crafted input samples. This paper presents the results of a study to explore the use of Generative Adversarial Networks (GANs) in cyber security. The results obtained confirm that GANs enable the generation of synthetic malware samples that can be used to mislead a classification model.

Key words: cybersecurity, malware, artificial intelligence, machine learning, deep learning, generative adversarial networks

* Ppor. mgr inż. Michał Zimoń, Faculty of Cybernetics, Military University of Technology, Warsaw, e-mail: michal.zimon@wat.edu.pl.
** Płk dr inż. Rafał Kasprzyk, Faculty of Cybernetics, Military University of Technology, Warsaw, e-mail: rafal.kasprzyk@wat.edu.pl.

Introduction

Malware, or malicious software, is a major threat to cybersecurity. It can take many forms, including viruses, worms, and Trojan horses, and it can be used to steal sensitive information, disrupt systems, and spread to other devices. Traditional methods for detecting malware, such as signature-based detection and behavioural analysis, have their limitations and can be defeated by cleverly designed malware. As a result, researchers have explored alternative approaches, including the use of deep learning for detecting malware based on images of the code itself.

Deep learning is a subset of machine learning that uses artificial neural networks to automatically learn patterns and features in large datasets. It has been applied to various fields, including computer vision, natural language processing, and cybersecurity. In the context of malware detection, deep learning algorithms can analyse large amounts of data and identify patterns that are indicative of malware. These patterns may be present in the static characteristics of the malware, such as the code itself or the metadata associated with it.

Generating image representations of malware can potentially pose several dangers. One concern is that generating images of malware could facilitate the spread of malicious software. For example, if an image representation of malware is shared online, it could potentially be downloaded and executed by someone who is unaware of its true nature. This could lead to the unintentional installation of malware on a person's computer, potentially causing harm to the user and their data.

Another danger of generating image representations of malware is that it could potentially make it easier for malicious actors to bypass security measures. For example, if an image representation of malware is used as part of a phishing attack, it could potentially be more difficult for security systems to detect the malware, as it is not in its typical form. This could make it easier for attackers to successfully carry out their attacks and compromise the security of a system.

It is also important to note that generating image representations of malware could potentially raise legal and ethical concerns. Depending on the specific context, generating, and distributing image representations of malware could potentially be considered illegal or unethical, as it could facilitate the spread of harmful software.

Methodology

In our work, we want to check how the most popular classifiers trained on a dataset, containing a graphical representation of malware and benign software, will behave when they encounter those generated by GANs. We also used publicly available models to check how complex the process is.

Dataset

Both classifiers and generative networks were trained using the MaleVis[1] dataset. MaleVis is an open image dataset generated from 25 malware and 1 legitimate software class. Includes a total of 9,100 training and 5,126 validation RGB images at 224x224 or 300x300 resolution.

EfficientNet-B0

One of the networks used in our work for classification is Google's EfficientNet-B0[2]. It is part of the EfficientNet family of models that are designed to be highly efficient and work well across a variety of tasks and platforms. EfficientNet-B0 is a large model that has been trained on a dataset of millions of images and is intended for use in large-scale image classification tasks. It is characterized by high accuracy and performance, making it ideal for applications where computing resources are limited or where real-time performance is important.

EfficientNet-B0 is based on the MobileNetV2 architecture and uses a combination of depth wise separable convolutions and regular convolutions to build its model. It also includes several other techniques such as weight sharing and a composite scaling method to further improve performance and efficiency.

EfficientNet-B0 achieved top results in several image classification benchmarks, so it was further developed, and many subsequent versions were created. It is widely used in a variety of applications including object detection,

1 A.S. Bozkir, A.O. Cankaya, M. Aydos, *Utilization and Comparision of Convolutional Neural Networks in Malware Recognition*, 2019, https://www.researchgate.net/publication/331773587_Utilization_and_Comparision_of_Convolutional_Neural_Networks_in_Malware_Recognition [access: 4.01.2023].

2 M. Tan, Q. Le, *EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks*, 2019, https://arxiv.org/pdf/1905.11946.pdf [access: 4.01.2023].

image segmentation, and machine translation. It is also available as part of the TensorFlow-Slim library, making it easy to use and deploy in a variety of environments.

ResNet50

Another network used is ResNet50[3], developed by Microsoft Research. It is part of the ResNet family of models that are known for their deep architecture and ability to learn from large amounts of data efficiently. ResNet50 is a deep CNN that has been trained on a dataset of millions of images and is intended for use in large-scale image classification tasks. It has high accuracy and high performance in various benchmarks, making it a popular choice for a wide range of applications.

ResNet50 is built using a residual learning framework, which involves the use of shortcut connections that allow the network to learn residuals of the desired underlying mapping. This helps to alleviate the problem of vanishing gradients and enables the network to train deeper architectures without the performance degradation that often occurs with deeper networks. It also achieved state-of-the-art results on several tasks and usually competes with EfficientNet.

DCGAN

First network used to generate the samples is the Deep Convolutional Generative Adversarial Network[4]. It is a type of generative adversarial network (GAN) used for generating synthetic images. GANs consist of two neural networks: a generator and a discriminator. The generator is trained to produce synthetic samples that are indistinguishable from real ones, while the discriminator is trained to distinguish between real and synthetic samples. The two networks are trained in a zero-sum game, where the generator tries to fool the discriminator and the discriminator tries to correctly classify the samples as real or synthetic.

3 K. He et al., *Deep Residual Learning for Image Recognition*, 2015, https://arxiv.org/pdf/1512.03385.pdf [access: 4.01.2023].

4 A. Radford, L. Metz, S. Chintala, *Unsupervised Represenation Learning With Deep Convolutional Generative Aadversarial Networks*, 2016, https://arxiv.org/pdf/1511.06434.pdf [access: 4.01.2023].

DCGAN is a variant of GAN that uses convolutional neural network (CNN) architectures for both the generator and discriminator networks. This allows DCGAN to effectively capture the spatial dependencies and patterns in image data, making it well-suited for generating synthetic images.

DCGAN has been used to generate a wide range of synthetic images, including realistic images of faces, objects, and landscapes. It has also been used in a variety of applications, such as image synthesis, style transfer, and data augmentation. However, it is important to note that the synthetic images produced by DCGAN may not be representative of real-world images and should be used with caution.

StyleGAN2-ADA

Second network used to generate the samples is a variant of the StyleGAN2 generative adversarial network (GAN) architecture developed by NVIDIA. It is a state-of-the-art model for generating high-resolution, synthetic images and has been used to generate a wide range of images, including realistic images of faces, objects, and landscapes.

StyleGAN2-ADA is an extension of the original StyleGAN2 model that includes additional modifications and improvements, such as the use of adaptive discriminator augmentation (ADA) and a new truncation trick. These modifications allow StyleGAN2-ADA to generate even higher-quality images than the original StyleGAN2 model, while also improving the stability and efficiency of the training process.

It is a deep neural network that is trained using a large dataset of images. It can generate synthetic images by learning the underlying patterns and relationships in the training data. The generated images are highly realistic and are often difficult to distinguish from real ones.

StyleGAN2-ADA has been used in a variety of applications, including image synthesis, style transfer, and data augmentation. It is also widely used for research purposes, as it allows researchers to investigate the capabilities and limitations of GANs and other deep learning models.

Experiments

Classification

Last layers of both networks to classify the images were retrained using modified MaleVis dataset. To keep experiments quick, we first trained the networks for 5 epochs using Adam optimizer with learning_rate = 0.001. Then we recompiled the model with lower learning rate which was 0 and fine-tuned for 5 more epochs.

Dataset setting

For the classification between malware and benign software, 25 classes were considered as 1 class of malware. As a result, we got a dataset containing 1832 images representing normal software and 12394 images representing malware. Due to the disproportion of data, we decreased the number of malware samples. As a result, we used 1465 samples of benign software for training and 367 samples for validation and 1000 samples of malware for training, and 299 samples for validation. In addition, the images have been scaled to a resolution of 128 x 128 for faster training.

Performance

Source: own elaboration

Figure 1. EfficientNet-B0 training results

Source: own elaboration

Figure 2. ResNet50 training results

Table 1. Final performance of both networks

	Training		Validation	
	Loss	Accuracy	Loss	Accuracy
EfficientNet-B0	0.1833	0.9339	0.1150	0.9896
ResNet50	0. 0771	0.9813	0.1354	0.9583

GANs

DCGAN

Small amount of data made it hard to get satisfying results. We used DCGAN to generate benign samples based on dataset containing 1465 samples of benign software and 1000 samples of malware. Training process for benign samples was as follows:

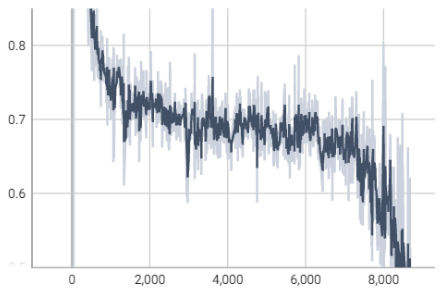


Figure 3. Discriminator loss (vertical) and steps (horizontal)

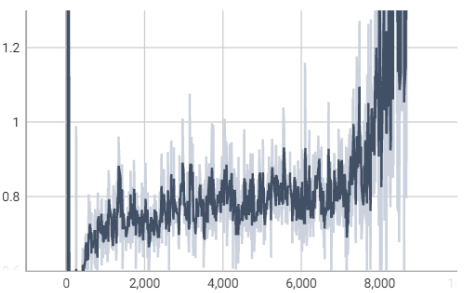


Figure 4. Generator loss (vertical) and steps (horizontal)

Samples from the trained generator:

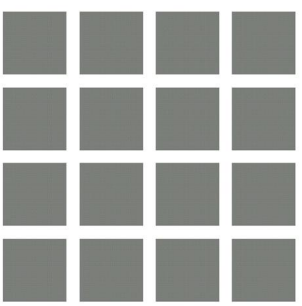


Figure 5. Epoch 0

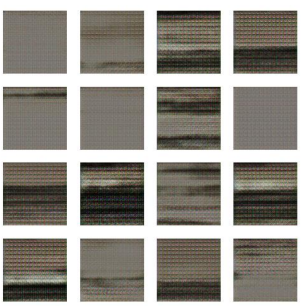


Figure 6. Epoch 100

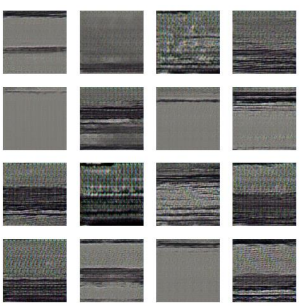


Figure 7. Epoch 290

Training on malware samples:

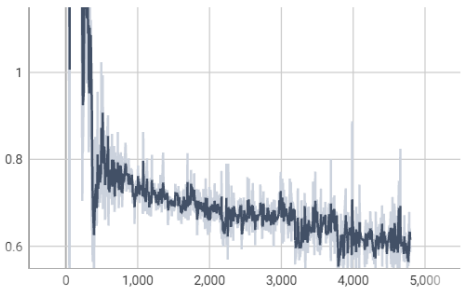


Figure 8. Discriminator loss (vertical) and steps (horizontal)

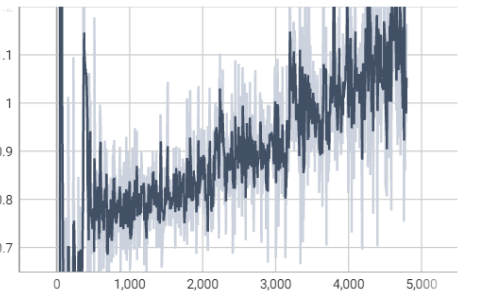


Figure 9. Generator loss (vertical) and steps (horizontal)

Generated samples:

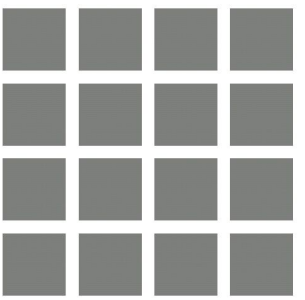


Figure 10. Epoch 0

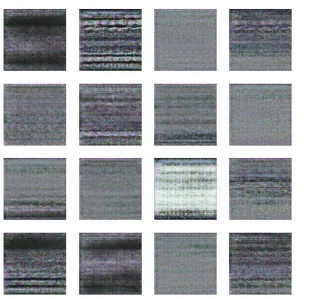


Figure 11. Epoch 100

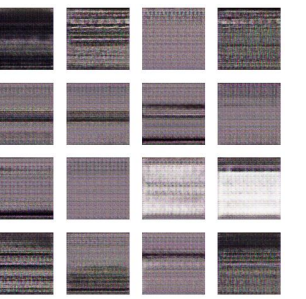


Figure 12. Epoch 290

Because dataset contains huge amount of malware samples, we also trained same network with dataset containing 12394 malware samples with batch_size = 64 and batch_size = 128. We got results as follows:

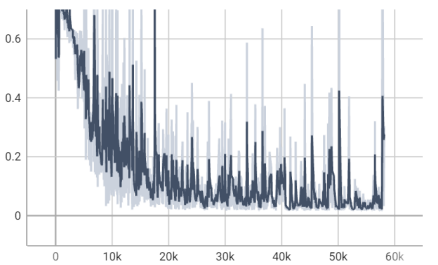


Figure 13. Discriminator loss (vertical) and steps (horizontal) for batch_size = 64

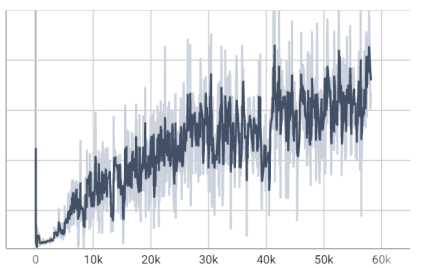


Figure 14. Generator loss (vertical) and steps (horizontal) for batch_size = 64

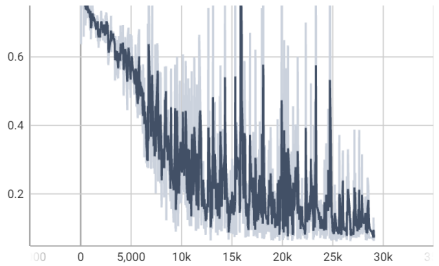


Figure 15. Discriminator loss (vertical) and steps (horizontal) for batch_size = 128

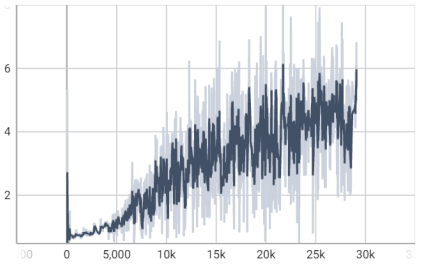


Figure 16. Generator loss (vertical) and steps (horizontal) for batch_size = 128

Generated samples:

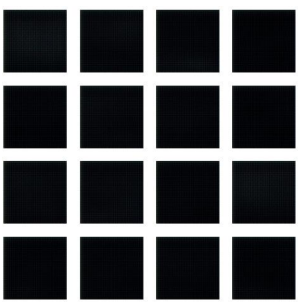


Figure 17. Epoch 0, batch_size 64

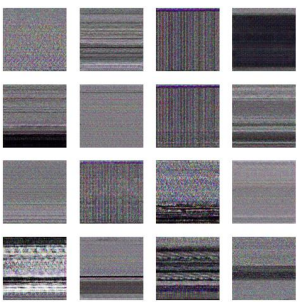


Figure 18. Epoch 100, batch_size 64

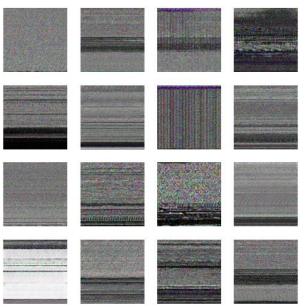


Figure 19. Epoch 290, batch_size 64

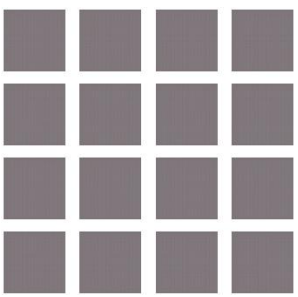


Figure 20. Epoch 0, batch_size 128

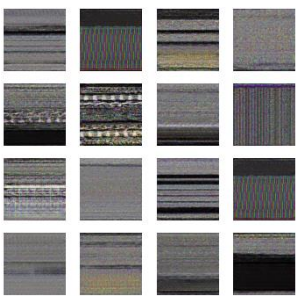


Figure 21. Epoch 100, batch_size 128

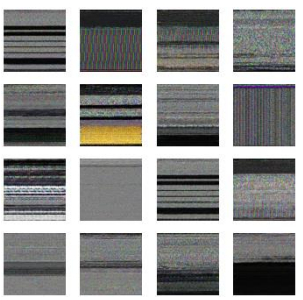


Figure 22. Epoch 290, batch_size 128

StyleGAN2-ADA

Authors of StyleGAN2-ADA proposed an adaptive discriminator augmentation mechanism that significantly stabilizes training process in limited data regimes. Because we had only 1832 samples of benign software and 12 394 of malware, we trained this network only to generate malware samples. Results of training process are as follows:

Figure 23. StyleGAN2-ADA training

After few days of training, we haven't seen any improvement. The best FID we achieved was 37.16 after epoch 19400. Generated samples during the training process:

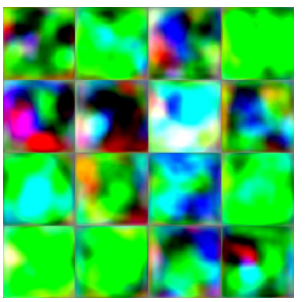


Figure 24. Epoch 0.

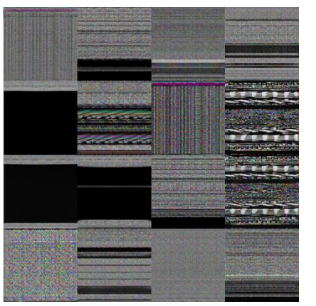


Figure 25. Epoch 19 400.

Figure 26. Epoch 25 000.

Results

After training generators from the different networks, we used them to generate 256 samples each of benign software and malware. First, we provided generated samples by DCGAN from reduced dataset as the input of previously trained networks for image classification. Results are shown in table below.

Table 2. Classification of generated samples for reduced dataset

	EfficientNet-B0		ResNet50	
	goodware	malware	goodware	malware
Goodware	256	0	256	0
Malware	208	48	240	16

Most of generated malware samples were misclassified as benign software. Situation looks better, when GANs were trained on 12 394 malware samples.

Table 3. Classification of generated samples for 12 394 malware samples

		Batch size	EfficientNet-B0		ResNet50	
			goodware	malware	goodware	malware
Malware	DCGAN	64	94	162	58	198
	DCGAN	128	105	151	76	180
	StyleGAN2-ADA	32	46	210	42	214

Conclusion

In this paper we showed how networks trained for image classification reacts to artificial samples which were generated. Accuracy during the training process and validation was high so such network could be used for malware detection. Surprisingly, we noticed problem with generating malware samples. Both EfficientNet-B0 and ResNet50 misclassified most of malware samples as benign software. Results were better with samples from StyleGAN2-ADA but still not perfect.

Too small dataset can be the cause of such behaviour. As mentioned in[5] it typically takes 50 000 to 100 000 training images to train a high-quality GAN. After all, malware is still software but designed to cause disruption to a target. Not enough samples may cause the situation where GAN simply is not able to learn the proper difference between malware and benign software. This may lead to generate a sample which will have software features but not the „malicious" part, hence it may be classified as benign software. Further work could be redoing the experiments on bigger dataset.

5 I. Salian, *NVIDIA Research Achieves AI Training Breakthrough*, 2020, https://blogs.nvidia.com/blog/2020/12/07/neurips-research-limited-data-gan/ [access: 4.01.2023].

On the other hand, GAN which will generate malware samples that can fool networks such as EfficientNet-B0 or ResNet50 and be classified as malware may rise several problems. Firstly, it will make it easier for malicious actors to attack security systems. Secondly, for both the malware and benign software it raises legal and ethical concerns. After all it is generated, not real sample, so should it be even considered as software?

Bibliography

Bozkir A.S., Cankaya, A.O., Aydos M., *Utilization and Comparision of Convolutional Neural Networks in Malware Recognition*, 2019, https://www.researchgate.net/publication/331773587_Utilization_and_Comparision_of_Convolutional_Neural_Networks_in_Malware_Recognition [access: 4.01.2023].

He K., Zhang X., Ren S., Sun J., *Deep Residual Learning for Image Recognition*, 2015, https://arxiv.org/pdf/1512.03385.pdf [access: 4.01.2023].

Karras T. et al., *Training Generative Adversarial Networks with Limited Data*, 2020, https://arxiv.org/pdf/2006.06676.pdf [access: 4.01.2023].

Radford A., Metz L., Chintala S., *Unsupervised Represenation Learning With Deep Convolutional Generative Aadversarial Networks*, 2016, https://arxiv.org/pdf/1511.06434.pdf [access: 4.01.2023].

Salian I., *NVIDIA Research Achieves AI Training Breakthrough*, 2020, https://blogs.nvidia.com/blog/2020/12/07/neurips-research-limited-data-gan/ [access: 4.01.2023].

Tan M., Le Q., *EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks*, 2019, https://arxiv.org/pdf/1905.11946.pdf [access: 4.01.2023].

Jeszcze jedna praca badawcza dotycząca sieci GAN w cyberbezpieczeństwie

Streszczenie

Algorytmy głębokiego uczenia pozwoliły osiągnąć znakomite wyniki w różnorodnych zadaniach, w tym w klasyfikacji obrazów, tłumaczeniu języka, rozpoznawaniu mowy i cyberbezpieczeństwie. Mogą one uczyć się złożonych wzorców i zależności z dużych ilości danych, dlatego są bardzo skuteczne w wielu zastosowaniach. Jednakże ważne jest to, żeby zdawać sobie sprawę, że modele zbudowane z wykorzystaniem uczenia głębokiego nie są niezawodne i można je oszukać za pomocą starannie przygotowanych próbek wejściowych. W artykule zostały przedstawione wyniki badań, których celem jest zbadanie możliwości wykorzystania generatywnych sieci antagonistycznych (ang. Generative Adversarial Networks – GAN) w cyberbezpieczeństwie. Uzyskane wyniki potwierdzają, że sieci GAN umożliwiają generowanie syntetycznych próbek złośliwego oprogramowania, które mogą zostać wykorzystane do wprowadzenia w błąd model klasyfikacyjny.

Słowa kluczowe: cyberbezpieczeństwo, złośliwe oprogramowanie, sztuczna inteligencja, uczenia maszynowe, głębokie uczenie, generatywne sieci antagonistyczne

Paweł Pelc*

The Polish Financial Supervision Authority in the national cybersecurity system

Abstract

The Polish Financial Supervision Authority is the authority competent for cybersecurity for the banking sector and financial market infrastructure. It is the only cybersecurity authority that does not have the status of a minister managing a government administration department as well as being the only authority competent for cybersecurity outside the structure of the government administration and not operating within the legal personality of the State Treasury. Only some entities supervised by the Polish Financial Supervision Authority under the regulations on supervision over the financial market are subject to its supervision as the authority competent for cybersecurity. Regulatory differences lead to the necessity to apply different rules when the Polish Financial Supervision Authority carries out controls under the regulations on financial market supervision and controls under the National Cybersecurity System Act.

Key words: The Polish Financial Supervision Authority, supervisory authority, administrative authority, national cybersecurity network

* Paweł Pelc, War Studies University in Warsaw, Academic Centre for Cyber Security Policy, e-mail: pawel.pelc@gmail.com, ORCID: 0000-0002-5007-568X.

Existing since 2006, the Polish Financial Supervision Authority – an integrated financial market regulator[1] – upon the entry into force on 28 August 2018 of the National Cybersecurity System Act of 5 July 2018[2] – became the authority competent for cybersecurity for the banking sector and financial market infrastructure, in accordance with Art. 41(4) thereof. None of these terms are defined in the glossary to the National Security System Act contained in Art. 2 Annex 1, describing sectors and subsectors and types of entities, defines the „Banking and Financial Market Infrastructure" sector, which includes credit institutions, domestic banks, branches of foreign banks, branches of credit institutions, credit unions, a regulated market operator, a CCP (a legal person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer), and a joint stock company that is a subsidiary of the National Securities Depository, to which the National Securities Depository has delegated by written agreement the performance of its statutory tasks. Despite the use of the term „banking sector and financial market infrastructure sector" in Art. 41(4) of the National Cybersecurity System Act, and the definition of the sector in Annex 1 thereto, referred to as „Banking and financial market infrastructure" which would lead to the conclusion that these are not the same concepts, the only rational interpretation is to determine that in both cases the scope of regulation is the same. Indeed, it should be pointed out that neither the term 'banking sector' nor the term „financial market" are explicitly defined in the Act of 21 July 2006 on financial market supervision[3]. This Act only defines, in Art. 1(2)(1), banking supervision by referring to the regulations of the Banking Law[4], the Act of 29 August 1997 on the National Bank of Poland[5], the Act of 29 August 1997 on Mortgage Bonds and Mortgage Banks[6], the Act of 7 December 2000 on the Operation of Cooperative Banks[7]

1 P. Pelc, *The Polish Financial Supervision Authority in the Polish administrative system*, „Cybersecurity and Law" 2022, no. 2.

2 Consolidated text, Journal of Laws 2022, item 1863.

3 Consolidated text, Journal of Laws 2022, item 660. Cf. P. Pelc, *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, no. 2, p. 152–153.

4 The Act of 29 August 1997 – the Banking Law, consolidated text, Journal of Laws 2021, item 2439.

5 Consolidated text, Journal of Laws 2022, item 2025.

6 Consolidated text, Journal of Laws 2022, item 581.

7 Consolidated text, Journal of Laws 2022, item 1595.

and the EU Regulation on Prudential Requirements for Credit Institutions[8]. The reference to the scope of banking supervision contained in the Act on Financial Market Supervision is additionally flawed in that there is no separate supervision over financial market infrastructure. Under the Act on Financial Market Supervision, the entities listed in Annex 1 to the National Cybersecurity System Act are subject not only to banking supervision but also to capital market supervision and supervision over credit unions. If the reference to the regulations of the Act on Financial Market Supervision does not allow proper reconstruction of the scope of the term 'banking and financial market infrastructure sector', and this term is not separately defined in Article 2 of the National Cybersecurity System Act, as well as the meaning of this term cannot be clearly determined using the linguistic meaning of this term, the only reasonable possibility to determine the meaning of the provision set out in Art. 41(4) of the National Cybersecurity System Act is to interpret it following the wording of Annex 1 thereto and assume that the term „banking sector and financial market infrastructure" should be construed as the Banking and Financial Market Infrastructure sector. This leads to the conclusion that the Polish Financial Supervision Authority is the authority competent for cybersecurity not for all entities that are subject to its supervision under the Act on Financial Market Supervision, but only for entities that are part of the Banking and Financial Market Infrastructure Sector, pursuant to Annex 1 to the National Cybersecurity System Act. According to the Report on the activities of the UKNF (Polish Financial Supervision Authority) and the KNF Board (Board of the Polish Financial Supervision Authority) in 2018[9] in accordance with Art. 86 of the National Cybersecurity System Act, „the KNF Board identified, by 9 November 2018, 19 entities representing the banking sector and financial market infrastructure which met the criteria for recognition as operators of essential services, and issued the related decisions"[10]. In the following years, the KNF Board issued decisions regarding further two entities, as well as two decisions on the expiration of the decision to recognise an entity as an

8 Regulation (EU) 575/2013 of the European Parliament and of the Council of 26 June 2013 on Prudential Requirements for Credit Institutions and Investment Firms and amending Regulation (EU) No 648/2012, Official Journal of the European Union 2003, L 176.

9 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018 roku*, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%20z%20dzia%C5%82alno%C5%9Bci%20UKNF%20oraz%20KNF%20w%202018%20roku_66979.pdf [access: 4.10.2022].

10 Ibidem, p. 193.

operator of essential services, therefore, as of the end of 2021, there were 19 entities recognised as operators of essential services by the KNF Board as an authority competent for cybersecurity, with 15 entities belonging to the banking and credit union sector and 4 entities belonging to the financial market infrastructure sector[11].

Entrusting the Polish Financial Supervision Authority with the role of an authority competent for cybersecurity is an unusual solution on the grounds of Art. 41(1–3) and (5–11) of the National Cybersecurity System Act because it is the only authority competent for cybersecurity that does not have the status of minister (the other authorities competent for cybersecurity are the ministers competent for energy, transport, maritime economy, inland navigation, health, water management, computerisation and the Minister of National Defence)[12]. Thus, all other authorities competent for cybersecurity have the status of a constitutional minister heading a government department[13], are part of the Council of Ministers and form part of the government administration, and operate under the legal personality of the State Treasury. In the case of the Polish Financial Supervision Authority, the situation is different, it is admittedly a public administration body, but it is not a government administration body, it is not part of the Council of Ministers, nor does it head a government administration department. In addition, as of 1 January 2019, the UKNF became a state-owned legal person, and the KNF Board – its body, that is – began to function outside the scope of the legal personality of the State Treasury[14].

11 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020 r.*, Warszawa 2021, p. 136, https://www.knf.gov.pl/knf/pl/komponenty/img/SPRAWOZADANIE%202020_76375.pdf [access: 4.10.2022]; *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 r.*, p. 150–151, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf [access: 4.10.2022].

12 More extensively on the tasks of the Minister of National Defence: K.A. Wąsowski, *Cognition of the Minister of National Defence in the scope of cybersecurity*, „Cybersecurity and Law" 2019, no. 1, p. 11–24; M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, ibidem 2022, no. 1, p. 85–94.

13 Cf. A. Brzostek, *Organy właściwe do spraw cyberbezpieczeństwa* [in:] *System cyberbezpieczeństwa*, Warszawa 2021, p. 200–202.

14 P. Pelc, *The Polish…*; M. Torończak, *Kilka uwag na temat nowej konstrukcji nadzoru nad rynkiem finansowym*, „Monitor Prawniczy" 2019, no. 10, p. 537; A. Nadolska, *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

According to Art. 41 of the National Cybersecurity System Act, an authority competent for cybersecurity (which also means the Polish Financial Supervision Authority with respect to the banking and financial market infrastructure sector): 1) analyses, on an ongoing basis, entities in a given sector or sub-sector in terms of recognising them either as an operator of essential services or non-compliance with the conditions qualifying a given entity as an operator of essential services; 2) issues decisions recognising a given entity as an operator of essential services, or decisions confirming the expiration of the decision recognising a given entity as an operator of essential services; 3) immediately after issuing a decision recognising a given entity as an operator of essential services or a decision confirming the expiration of the decision recognising a given entity as an operator of essential services, submits applications to the minister competent for computerisation to enter that entity in the list of operators of essential services or to remove it from that list; 4) submits applications to change data in the list of operators of essential services, not later than within six months from the change of these data; 5) prepares, in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams, recommendations on actions aimed at strengthening cybersecurity, including sectoral guidelines on incident notifications; 6) monitors the application of the provisions of the Act by operators of essential services and digital service providers; 7) requires operators of essential services or digital service providers, at the request of CSIRT NASK, CSIRT GOV or CSIRT MON, to remove, within the prescribed period, the vulnerabilities that have led or could lead to a serious, significant or critical incident; 8) conducts inspections of operators of essential services and digital service providers; 9) may cooperate with the competent authorities of EU Member States via the Single Point of Contact; 10) processes information, including personal data, about the essential and digital services being provided and the operators of essential services or digital service providers to the extent necessary to perform the tasks provided for in the Act; 11) participates in cybersecurity exercises organised in the Republic of Poland or in the European Union.

On the other hand, there are doubts about the possibility to apply to the Polish Financial Supervision Authority the powers under Art. 41(3) to (6) of the National Cybersecurity System Act to entrust, on its behalf, the performance of some of these tasks to units subordinate to or supervised by it, which results from the separateness of the Polish Financial Supervision Authority from the other authorities competent for cybersecurity. The Polish Financial

Supervision Authority has no subordinate units, and only supervises financial market entities. For these reasons, despite the absence of an explicit provision excluding the application of Art. 41(3) of the National Cybersecurity System Act to the Polish Financial Supervision Authority, it should be considered inapplicable to the Polish Financial Supervision Authority for the above reasons. The National Cybersecurity System Act provides that in justified cases the authorities competent for cybersecurity, and this means the Polish Financial Supervision Authority too, shall cooperate with law enforcement agencies and the authority competent for the protection of personal data. It should be pointed out that, according to Art. 16(5) of the Act on Financial Market Supervision, giving notice of a suspected criminal offence or providing further information in addition to this notice shall not violate the obligation of professional secrecy, while based on the regulation on professional secrecy, cooperation with law enforcement agencies may raise problems if this would require the provision of information covered by professional secrecy without giving notice of a suspected criminal offence as long as these would be other authorities than those specified in Art. 17ca of the Act on Financial Market Supervision. The authorities competent for cybersecurity, including the Polish Financial Supervision Authority, are authorised to obtain information under the rules laid down in Art. 43 of the National Cybersecurity System Act, as well as establish a sectoral cybersecurity team under Art. 44 of the National Cybersecurity System Act.

Pursuant to Art. 53 of the National Cybersecurity System Act, the authorities competent for cybersecurity, including the Polish Financial Supervision Authority, exercise supervision[15] within the scope of the compliance with the provisions of the National Cybersecurity System Act concerning the performance by operators of essential services of their obligations imposed under the National Cybersecurity System Act regarding counteracting cybersecurity threats and reporting serious incidents, as well as meeting by digital service providers the requirements regarding the security of the digital services they provide, as specified in Implementing Regulation 2018/151 and the performance of the obligations provided by the Act for reporting significant incidents. They may conduct inspections in this regard and impose fines on operators of essential services and digital service providers.

15 M. Nowikowska, *Nadzór i kontrola operatorów usług kluczowych, dostawców usług kluczowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*, „Cybersecurity and Law" 2021, no. 1, p. 77–103.

Control in respect of entities that are enterprises is subject to the provisions of Chapter 5 the Act of 6 March 2018 – the Enterprise Law[16], whilst the National Cybersecurity System Act further specifies the obligations of controlled enterprises, the evidence procedure during the control which is carried out by persons performing inspection activities, and it also regulates issues related to control reports with post-control recommendations. In contrast, the National Cybersecurity System Act does not provide for the application of regulations regarding control carried out by the Polish Financial Supervision Authority of supervised entities in this regard. It should be recognised that the regulation in Art. 53–59 of the National Cybersecurity System Act is of a special nature in respect of the regulations regarding control carried out by the Polish Financial Supervision Authority in supervised entities contained in the regulations on particular types of entities supervised under the Act on Financial Market Supervision.

Under Art. 86 of the National Cybersecurity System Act, the authorities competent for cybersecurity, including the Polish Financial Supervision Authority, were required, by 9 November 2018, to issue a decision on recognising an operator of essential services and to submit to the Minister competent for computerisation applications to include operators of essential services in the list of operators of essential services. The Polish Financial Supervision Authority fulfilled this obligation on time[17].

On 1 April 2019 the Cybersecurity Department was established within the UKNF's organisational structure „responsible for 1) the supervision of financial market entities in the area of ICT risk and cybersecurity in terms of financial market supervision; 2) the performance of tasks under the National Cybersecurity System Act of 5 July 2018 [...]; 3) undertaking measures to ensure a high level of cybersecurity at the UKNF"[18].

In addition, on 1 July 2020, the KNF Board as an authority competent for cybersecurity established the KNF CSIRT acting as the Sectoral Team for Cybersecurity to coordinate activities and support the management

16 Consolidated text, Journal of Laws 2021, item 162.

17 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018*..., p. 193.

18 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2019 r*., Warszawa 2020, p. 140, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%202019.pdf [access: 4.10.2022].

of security incidents of financial market entities recognised as operators of essential services[19].

According to the information provided by the UKNF, the KNF Board has effectively stepped into the role of an authority competent for cybersecurity in accordance with the regulations of the National Cybersecurity System Act, whilst its different nature from other authorities competent for cybersecurity does not have an adverse impact on fulfilling this role. Given its role as a financial market regulator, the Polish Financial Supervision Authority should be considered a body well-prepared to carry out supervisory and control functions on the grounds of the National Cybersecurity System Act, irrespective of the regulatory differences between the regulations on financial market supervision and controls carried out within this supervision, and the supervision it exercises as the authority competent for cybersecurity and controls carried out under the National Cybersecurity System Act.

Bibliography

Brzostek A., *Organy właściwe do spraw cyberbezpieczeństwa* [in:] *System cyberbezpieczeństwa*, Warszawa 2021.

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Nadolska A., *Soft law w regulacji rynku finansowego w Polsce: rekomendacje, wytyczne i lista ostrzeżeń publicznych KNF*, Warszawa 2021.

Nowikowska M., *Nadzór i kontrola operatorów usług kluczowych, dostawców usług kluczowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa*, „Cybersecurity and Law" 2021, no. 1.

Pelc P., *Tajemnica zawodowa w instytucjach rynku finansowego w kontekście polskich regulacji dotyczących cyberbezpieczeństwa*, „Cybersecurity and Law" 2019, no. 2.

Pelc P., *The Polish Financial Supervision Authority in the Polish administrative system*, „Cybersecurity and Law" 2022, no. 2.

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2018 r., Warszawa 2019, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie%20z%20dzia%C5%82alno%C5%9Bci%20UKNF%20oraz%20KNF%20w%202018%20roku_66979.pdf [access: 4.10.2022].

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020 r., Warszawa 2021, https://www.knf.gov.pl/knf/pl/komponenty/img/SPRAWOZADANIE%202020_76375.pdf [access: 4.10.2022].

Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 r., https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf [access: 4.10.2022].

19 *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2020...*, p. 137; *Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021...*, p. 151–154.

Torończak M., *Kilka uwag na temat nowej konstrukcji nadzoru nad rynkiem finansowym*, „Monitor Prawniczy" 2019, no. 10.
Wąsowski K.A., *Cognition of the Minister of National Defence in the scope of cybersecurity*, „Cybersecurity and Law" 2019, no. 1.

Komisja Nadzoru Finansowego w krajowym systemie cyberbezpieczeństwa

Streszczenie

Komisja Nadzoru Finansowego jest organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych. Jest to jedyny organ właściwy do spraw cyberbezpieczeństwa, który nie ma statusu ministra kierującego działem administracji rządowej i jednocześnie jest to to jedyny organ właściwy do spraw cyberbezpieczeństwa znajdujący się poza strukturą administracji rządowej i nie działający w ramach osobowości Skarbu Państwa. Jedynie część rodzajów podmiotów nadzorowanych przez Komisję Nadzoru Finansowego na gruncie regulacji o nadzorze nad rynkiem finansowym podlega jej nadzorowi jako organu właściwego do spraw cyberbezpieczeństwa. Odmienności regulacyjne prowadzą do konieczności stosowania odmiennych zasad w trakcie przeprowadzania przez Komisję Nadzoru Finansowego kontroli na podstawie regulacji dotyczących nadzoru na rynkiem finansowym i kontroli na podstawie ustawy o krajowym systemie cyberbezpieczeństwa.

Słowa kluczowe: Komisja Nadzoru Finansowego, organ nadzoru, organ administracji publicznej, krajowy system cyberbezpieczeństwa

András Bencsik*
Mirosław Karpiuk**

Cybersecurity in Hungary and Poland. Military aspects

Abstract

Nowadays, ensuring cybersecurity is an important objective of public authority. It must take into account the protection of cybersecurity, both in the current and future perspectives. The state security policy must also take into account its dimension in cyberspace, especially today, where many services are provided through communication and information systems.

A special place in the cybersecurity system is given to cyberspace security in the military dimension. In this regard, both the military administration and civil law entities, both acting for defence, will be competent. Effective military operations are directly linked to new digital technologies. As a result, for the sake of state security (both internal and external), it becomes necessary not only to respond to cyberattacks, but also to counteract them.

Key words: cybersecurity, cyberspace, armed forces, the Minister of National Defence

* Assoc. Prof. András Bencsik, PhD, associate professor of Administrative Law, Faculty of Law, Eötvös Lóránd University, e-mail: bencsik.andras@ajk.elte.hu, ORCID: 0000-0001-5772-9968.

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

Introduction

In a digital state, communication and information systems become particularly important. They provide not only fast communication, but also aid in the provision of services or the performance of tasks. They are used for a variety of purposes, from entertainment, through communication, education and work, through to digital security. From the perspective of the normal functioning of the state, it is important not only to perform tasks with the use of cyberspace, but also to ensure cybersecurity, including in military terms. The protection of cyberspace must be continuous, not only during crises or conflicts (although especially in these cases) but also when the state is performing its tasks uninterruptedly.

Due to the need to ensure cybersecurity (including that in military terms), knowledge, skills and competencies from the sphere of digital threats, cybersecurity risk management, the protection of information systems and critical infrastructure are required. Professional staff carrying out cybersecurity tasks, with the right knowledge, the right skills, or the right competences, can guarantee the quality of activities protecting cyberspace, contributing to the optimisation of its operation and minimising disruptions occurring in this area.

Particular attention should be paid to the need to increase the resilience of information systems that are used in the military sphere, and as such exposed to cyber threats. Seeking to achieve a level of protection that ensures the uninterrupted operation of information systems must be an important direction of the national defence policy.

In the military sphere, an invaluable role is played by the national cybersecurity system, the purpose of which is to ensure cybersecurity at a national level, including the uninterrupted provision of essential services and digital services, by achieving an adequate level of security of the information systems used to provide these services and ensuring incident handling[1]. Nowadays, cyberspace as an operational domain plays an important role for both offensive and defensive operations, and it must be properly secured, especially against cyber-attacks on critical infrastructure aimed at destabilising the state.

1 Art. 3 of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2020, item, 1369, as amended.), hereinafter: the NCSA.

Military aspects of cybersecurity in Hungary

The public administration (including its organisational structure, its operational mechanisms and its staffing framework) does not (or cannot) remain unchanged, cannot be independent of the trends of the contemporary world, and thus it can be said that public administration is constantly in flux. One of the major challenges of our time is digitalisation in the broadest sense, which has required a reorganisation of both the public administration's approach to citizens and its infrastructure in all the countries of the world.

For the sake of completeness, however, the authors of this paper cannot fail to highlight the undisputed virtues of optimal digitisation of public administration, which are also relevant to our study. The leading foreign literature is unanimous in the view that the use of proven digital tools can have a pull effect, which can legitimise the use of new technological tools in new sectors not previously affected by digitisation. This effect is reinforced by the fact that standardised platforms and other digital solutions from the competitive sector can be easily transferred to public administrations, within certain scope and under certain conditions. In fact, this intermediary, interactive online value creation is a phenomenon also known in the „traditional" offline economy, which generally operates on the technology and infrastructure of a business[2]. On the other hand, it should also be stressed that technological tools can be used to a greater extent to achieve and reinforce the objectives declared as goals to be achieved by national and EU public administration policy (e.g. customer focus, efficiency, subsidiarity, etc.), particularly with regard to the activities of public authorities and the organisation of public services. In this context, we would refer to the indicators of the Digital Economy and Society Index (DESI), which ranks the countries of the Central and Eastern European Union in the bottom third of the scale, particularly in terms of the efficiency of public services[3]. It should also be pointed out, however, that digitisation is not just a matter of the functioning of the state and the development of public services: in addition to civil administration, the use

2 On the competition law aspects of this, see J. Firniksz, *Rangsorolation – a new regulatory issue in the age of platforms and information supply*, https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf [access: 31.07.2022].

3 https://digital-strategy.ec.europa.eu/en/policies/desi [access: 31.07.2022]. According to the index, Hungary ranks 23rd, Slovakia 24th, Poland 25th and the Czech Republic 18th, with slightly better indicators.

of new technologies is also becoming increasingly important in defence administration (including defence and the conduct of military operations). There are legal, IT and military aspects to this, which are worth examining and which could also be used to fine-tune the regulatory environment.

It is also worth pointing out that, however inevitable the emergence of the digital explosion in the public sector may be, experience to date – especially in the CEE region – does not necessarily suggest that it is a complete success story. The reasons for this include the difficulty of taking organisational and procedural aspects into account at the same time, the slow and costly process of building infrastructure, and the general resistance to change (especially in human resources), which is also a classic barrier to innovation[4]. Unfortunately, the military-defence aspect, which is the narrower subject of this study, has, however, extensive experience and international reactions, which show that cyberspace is (has been) more receptive to the application of the technologies indicated than civil administration[5].

The military aspects of cyber defence have become an inescapable priority in the framework of NATO (and Hungary as part of it) defence management. Behind this trend is the realisation that, following the end of the Cold War, cybersecurity activities pose the greatest risk, with cyber warfare emerging as a new phenomenon, with operational effects in cyberspace[6]. The question rightly arises as to what are the specific characteristics of cyber warfare that justify a completely new basis for defining the nature of military operations (and defence). There seems to be a consensus in the authoritative literature that the defining characteristics of cyber warfare are: 1) there are no national borders (this is essentially a consequence of the borderless nature of cyberspace and the diversity of attacks); 2) the warring parties include not only military but also civilian actors (espionage, disruptive or destructive goals are often achieved through the involvement of hacker groups); 3) participants

4 Another unfortunate development is that in Hungary there have recently been several articles which, in addition to presenting the results achieved, emphasise why there is no need or opportunity for further digitisation in public administration. Among others, the study by Erzsébet Fejes and Iván Futó, cited later, can be mentioned in this context.

5 In this context see K. Fekete-Krydis, B. Lázár, *Military Defence*, „Review" 2020, no. 3, p. 44.

6 Cf. T. Tóth, *Introducing the NATO Cyber Defence Centre of Excellence*, „National Security Review" 2018, no. 4, p. 49.

and destinations include international companies, domestic and international service providers and global services[7].

Hungary has been a member of the North Atlantic Treaty Organisation (NATO) since 1999, and therefore Hungary could not have been unaffected by the trends and reactions that have emerged in recent years in relation to cyber warfare within NATO. NATO was confronted with cyber warfare for the first time this year, following the bombing of Kosovo, and the cyberattacks detected were carried out initially by the Serbian hacker group Black Hand, and then by Chinese and Russian hackers following the bombing of the Chinese Embassy. The story had both indirect and direct international consequences. The following developments are worth highlighting: 1) following the 2002 NATO summit in Prague, the development of a NATO cyber defence policy came to the fore[8]; 2) at the 2014 Wales Summit, NATO's cyber defence policy guidelines were adopted and cyber defence was included in the collective defence tasks[9]; 3) in 2016, in the final document of the Warsaw Summit, the Allies extended the scope of operational warfare to cyberspace and declared that a cyberattack against a NATO member state could be considered an attack against the Alliance as a whole and could be subject to collective response if necessary[10]; 4) at the 2018 Brussels Summit, it was declared that, while NATO is focused on developing collective defence cyber capabilities, member states are building a full range of capabilities for deterrence and effective action[11].

For reasons of scope, this study cannot provide an overview of NATO's cyber defence activities, so we will now focus on the legislative developments made by the Hungarian legislator to achieve the Alliance's objectives. Among the Hungarian legislative developments, the present study will focus on a relatively new piece of legislation catalysed by NATO's cyber defence policy,

7 See *Cyber warfare and military cyber defence*, https://11686cc6-54a5-8388-87db-54233ab8a32d [access: 22.11.2022].

8 For more on this, see A. Tóth, *Resolutions and agreements following the Prague NATO Summit on the modernisation of the command and control system and the development of joint operational capability*, „Hadmérnök" 2016, no. 3, p. 214.

9 Wales Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, https://www.nato.int/cps/en/natohq/official_texts_112964.htm [access: 23.11.2022.]

10 Warsaw Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm [access: 23.11.2022].

11 Brussels Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm [access: 23.11.2022].

namely Act L of 2013 on the Electronic Information Security of State and Local Government Bodies.

The rationale behind the adoption of the legislation is essentially based on the recognition that Hungary, like many other countries in the world, considers cybersecurity a national security issue of high priority[12]. The legislation is both new and old: while it can be noted that information security regulation in Hungary dates back 30 years, the legislative product under consideration can be considered novel in several respects. In this respect, the novae can be identified below: 1) no legislation had previously regulated the IT security of public administrations; 2) since then, there has been a separate regulation on critical infrastructure protection, with which the protection of critical information infrastructure fits in; 3) there have been bodies in the past that have (also) dealt with cyber defence, without a legal basis, in the absence of regulation[13].

The legislation has been the subject of serious professional-political debates in the literature and (in the legislative debate) among certain opposition parties, even before it is actually applicable. One of the most serious concerns is the scope of the law, since at the time of its adoption there was no inventory of critical information infrastructures, which meant that the legislator was forced to designate these actors, in terms of legal security[14].

The other key issue of the reservations is the so-called „Big Brother" effect, the real risk of which is not yet supported by a legal context: on the one hand, it should be stressed that the authorities have had legal means to monitor the electronic activities of certain citizens, and on the other hand, according to some representatives of the literature[15], it is precisely a properly functioning information security system that can provide a control that can strengthen the transparency of organisations.

From the discussion presented in this short paper, it is clear that the Act will result in a forced redesign in the state and local government sector, with the legislator's not hidden aim of providing a predictable path for the organisations

12 Cf. C. Krasznay, L. Muha, *Cyber defence in Hungary: a blessing or a curse?*, „HWSW Online IT News Magazine" 2013, no. 3.

13 Here we mention the National Security Service, of which the National Cyber Defence Institute is now part.

14 This obligation was fulfilled by the legislator with the creation of Government Decree No. 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and installations.

15 In this context see C. Krasznay, L. Muha, op. cit.

concerned, on the one hand, and (in justified cases) the possibility of immediate intervention, on the other hand, if the inadequate operation of an organisation in cyberspace is objectionable for reasons of national security.

Military aspects of cybersecurity in Poland

The development of new technologies, including military ones, contributes to a significant increase in the employment of unmanned and autonomous systems, automated and robotised weapon platforms using artificial intelligence, as well as long-range precision weapon systems, including ballistic and cruise missiles. Digital technologies are advancing dynamically, which creates the necessity for their efficient use. The development of solutions based on fixed and mobile broadband networks, and artificial intelligence, creates new development opportunities, whilst unfortunately creating previously unknown threats. The challenge for the state is to join the technological race in this area[16]. Conducting military operations (of a defensive nature) in cyberspace is a fundamental task of the state, including military administration. These measures must be adequate to the degree of the threat, must keep up with the dynamics of the development of new technologies used in this sphere, including the use of modern solutions applicable in the world, in order not only to effectively combat cyber threats, but also to prevent them. Civilian actions taken in cyberspace also need to correspond to the dynamics of the development of new technologies in cyberspace, as this also translates into the efficiency of the state and its institutions in carrying out public tasks.

Cybersecurity, as defined in Art. 2(4) of the NCSA, is the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[17]. In the case of military cybersecurity,

16 *National Security Strategy of the Republic of Poland*, Warszawa 2020, p. 7–8. See also M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, s. 49.

17 For more information about cybersecurity refer to: W. Pizło, *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Karpiuk, *Activities of local government units in the scope of telecommunication*,

information systems will be used by military entities, and civilian ones to the extent in which they work for defence.

Ensuring cybersecurity is one of the basic tasks of public authorities, especially due to the fact that threats of an IT nature are increasingly dangerous and cyberattacks can be used as a means of political pressure[18]. The implementation of this task can take place in the military sphere, and it may involve the use of military telecommunications systems.

One of the authorities competent for cybersecurity in the military sphere is the Minister of National Defence. The Minister of National Defence manages the national defence department which, during peacetime, handles the following issues: 1) the defence of the state and the Armed Forces of the Republic of Poland; 2) cyberspace security in the military dimension; 3) the participation of the Republic of Poland in the military undertakings of international organisations and in the discharge of military obligations under international agreements; 4) offset agreements[19]. In the military sphere, the Minister of National Defence is the executive body in matters relating to ensuring cybersecurity. He performs tasks in this regard through subordinate and supervised organisational units.

The Armed Forces of the Republic of Poland, being a core element of the state's defence system, should engage in cyberspace operations at the same level as they do in their in air, land and sea operations, in peacetime, war and in crisis situations. Cyberspace activities undertaken by the military must include

„Cybersecurity and Law" 2019, no. 1; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2; M. Karpiuk, *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1; M. Czuryk. *Special rules of remuneration for individuals performing cybersecurity tasks*, ibidem, no. 2.

18 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, ibidem 2019, no. 1, p. 145.

19 Art. 19 of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended). See also M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1, p. 86–87.

identifying threats, protecting and defending ICT networks and systems, and combating sources of cyber threats[20].

Cyberspace security in the Armed Forces of the Republic of Poland is to be provided by the Cyberspace Defence Forces. They are a specialist component of the Armed Forces of the Republic of Poland and form a part thereof. They are tasked with performing the full spectrum of activities in cyberspace. In particular, this includes proactive protection and the active defence of elements and the resources of cyberspace relevant to the Armed Forces of the Republic of Poland[21].

Cyberspace Defence Forces are part of the Armed Forces of the Republic of Poland, but they are not a type of, but a component of, them. It should be mentioned here that the supreme Commander of the Armed Forces of the Republic of Poland is the President of the Republic of Poland. In peacetime he has command over the Armed Forces of the Republic of Poland through the Minister of National Defence[22].

Cyberspace (in which the Cyberspace Defence Forces operate) is construed as the space for processing and exchanging information created by communication and information systems, including relations between them and relationships with users[23]. In turn, a communication and information system is a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type[24].

Pursuant to Art. 23(1) of the AHD, the Defence Force Cyberspace Component Commander is competent to command military units and

20 Cybersecurity Strategy of the Republic of Poland – Annex to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazette of the Republic of Poland 2019, item 1037).

21 Art. 15(4) of the Act of 11 March 2022 on Homeland Defence (Journal of Laws 2022, item 655, as amended), hereinafter: the AHD.

22 Art. 134(1–2) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, no. 78, item 483, as amended), hereinafter: the Polish Constitution. See also M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3, p. 392.

23 See Art. 2(1b) of the Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws 2017, item 1932, as amended), hereinafter: the AML

24 Art. 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, Journal of Laws 2021, item 2070, as amended).

organised forces of the Cyberspace Defence Forces and is subordinate to: 1) the Minister of National Defence until the appointment of the Commander-in-Chief of the Armed Forces; 2) the Commander-in-Chief of the Armed Forces upon their appointment and their assumption of the command of the Armed Forces. A military unit is defined in Art. 2(12) of the AHD as an organisational unit of the Armed Forces of the Republic of Poland that operates on the basis of an established document issued by the Minister of National Defence and uses an official seal with the emblem of the Republic of Poland and the name (number) of the unit. In turn, an organised force, pursuant to Art. 2(38) of the AHD, means military units organised by the Minister of National Defence into a specific structure, in particular into a corps, division or brigade, operating independently or as part of a type of the Armed Forces of the Republic of Poland, on the basis of the establishment documents issued.

The subordination of the Armed Force Component Commander is explicitly stated in Art. 23(1) of the AHD. He is subordinated to the Commander-in-Chief of the Armed Forces. However, this function is not continuous. The President of the Republic of Poland, in coordination with the President of the Council of Ministers (upon his request), appoints him for the duration of the war. Consequently, he will function in the military structure of the state in the event of a special (qualified) security threat. In the event that the Commander-in-Chief of the Armed Forces has not been appointed, the Defence Force Cyberspace Component Commander is subordinated to the Minister of National Defence.

For the duration of war (the duration of warfare on the territory of the Republic of Poland), the President of the Republic of Poland appoints the Commander-in-Chief of the Armed Forces, as required under Art. 134(4) of the Constitution of the Republic of Poland[25]. From the perspective of the subordination of the Commander of the Cyberspace Defence Forces to the Commander-in-Chief of the Armed Forces, a mere appointment is not enough, as the latter must take command of the Armed Forces of the Republic of Poland.

As stipulated in Art. 23(2) of the AHD, the duties of the Defence Force Cyberspace Component Commander include in particular: 1) implementing the development programme of the Armed Forces of the Republic of Poland;

25 See also M. Kołodziejczak, *Funkcjonowanie Naczelnego Dowódcy Sił Zbrojnych w Rzeczypospolitej Polskiej*, Warszawa 2020, p. 65.

2) programming, planning, organising, conducting and supervising the training courses falling within the jurisdiction of the Defence Force Cyberspace Component Commander that are provided to the subordinate military units and organised forces, organisational cells and units, as well as institutions, bodies and entities, on the basis of concluded agreements; 3) planning and organising the development in the area of mobilisation and operation and the use of Cyber Defence Forces; 4) building, maintaining and protecting infrastructure, as well as protecting information in cyberspace; 5) conducting activities and operations in cyberspace; 6) providing support for military operations conducted by the Armed Forces of the Republic of Poland and operations in the allied and coalition system; 7) working in tandem with other bodies and entities in matters related to state defence; 8) managing and conducting inspections of subordinate military units and organised forces. The Defence Force Cyberspace Component Commander performs his tasks with the assistance of the Defence Force Cyberspace Component Command.

It should be pointed out that there is the need to develop the capabilities of the Armed Forces of the Republic of Poland to conduct operations in cyberspace. Due to the status of this formation, it is the Armed Forces that have the greatest obligation to provide cybersecurity in the military dimension. Hence, in order to meet this obligation, they must have adequate financial and legal resources, as well as adequate personnel.

Cybersecurity can also become a rationale for imposing martial law. According to Art. 2(1–1a) of the AML, in the event of an external threat to the state, including one caused by acts of a terrorist nature or acts in cyberspace, the President of the Republic of Poland may, at the request of the Council of Ministers, impose martial law on part or all of the state's territory. An external threat to the state is construed here as intentional actions which are detrimental to the independence and indivisibility of the territory, important economic interests of the Republic of Poland, or which aim to prevent or seriously disrupt the normal operation of the state, undertaken by entities that are external in relation to it.

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Cyber warfare and military cyber defence, https://11686cc6-54a5-8388-87db-54233ab8a32d [access: 22.11.2022].

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Fekete-Krydis K., Lázár B., *Military Defence*, „Review" 2020, no. 3.

Firniksz J., *Rangsorolation – a new regulatory issue in the age of platforms and information supply*, https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf [access: 31.07.2022].

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2.

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3.

Kołodziejczak M., *Funkcjonowanie Naczelnego Dowódcy Sił Zbrojnych w Rzeczypospolitej Polskiej*, Warszawa 2020.

Krasznay C., Muha L., *Cyber defence in Hungary: a blessing or a curse?*, „HWSW Online IT News Magazine" 2013, no. 3.

Pizło W., *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Tóth A., *Resolutions and agreements following the Prague NATO Summit on the modernisation of the command and control system and the development of joint operational capability*, „Hadmérnök" 2016, no. 3.

Tóth T., *Introducing the NATO Cyber Defence Centre of Excellence*, „National Security Review" 2018, no. 4.

Cyberbezpieczeństwo na Węgrzech i w Polsce. Aspekty militarne

Streszczenie

Zapewnienie cyberbezpieczeństwa stanowi obecnie ważny cel działania władzy publicznej. Musi ona ochronę cyberbezpieczeństwa uwzględniać w polityce zarówno bieżącej, jak i przyszłej. Polityka bezpieczeństwa państwa musi uwzględniać także cyberprzestrzeń, zwłaszcza obecnie, ponieważ wiele usług jest świadczonych za pośrednictwem systemów teleinformatycznych.

Szczególne miejsce w systemie cyberbezpieczeństwa zajmuje bezpieczeństwo cyberprzestrzeni w wymiarze militarnym. W tym zakresie będzie właściwa zarówno administracja wojskowa, jak i podmioty cywilne, ale działające na rzecz obronności. Skuteczne działania militarne są bezpośrednio związane z nowymi technologiami cyfrowymi. W związku z powyższym ze względu na bezpieczeństwo państwa (zarówno wewnętrzne, jak i zewnętrzne) konieczne staje się nie tylko reagowanie na cyberataki, lecz także im przeciwdziałanie.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, siły zbrojne, Minister Obrony Narodowej

Ewa Niewiadomska-Szynkiewicz*
Rafał Litka**

Ataki na urządzenia mobilne i metody ich wykrywania

Streszczenie

Indywidualna ochrona systemów autonomicznych z wykorzystaniem prostej analizy przesyłanych komunikatów staje się niestety niewystarczająca. Istnieje wyraźna potrzeba stworzenia nowych rozwiązań wykorzystujących dane z wielu źródeł, integrujących różne metody, mechanizmy ialgorytmy, w tym techniki przetwarzania Big Data i klasyfikacji danych wykorzystujące metody sztucznej inteligencji. Ilość, jakość, wiarygodność i aktualność danych i informacji o sytuacji w sieci oraz szybkość ich przetwarzania decydują o skuteczności ochrony. W pracy prezentowane są przykłady wykorzystania technik sztucznej inteligencji do wykrywania ataków na systemy teleinformatyczne. Uwaga koncentruje się na zastosowaniu metod uczenia maszynowego do detekcji złośliwych aplikacji instalowanych na urządzeniach mobilnych. Skuteczność przedstawionych rozwiązań została potwierdzona przez liczne eksperymenty symulacyjne przeprowadzone na rzeczywistych danych. Uzyskano obiecujące wyniki.

Słowa kluczowe: cyberbezpieczeństwo, detekcja ataków, aplikacje mobilne, sztuczna inteligencja, uczenie maszynowe, sztuczne sieci neuronowe, głębokie uczenie

* Prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz, kierownik Zespołu Złożonych Systemów, Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, e-mail: ewa.szynkiewicz@pw.edu.pl, ORCID: 0000-0003-4782-3816.
** Inż. Rafał Litka, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska, e-mail: rafal.litka.stud@pw.edu.pl.

Wstęp

Technologie informacyjne i komunikacyjne (ang. Information and Telecommunication Technologies – ITC) to obecnie jeden z podstawowych elementów decydujących o poziomie rozwoju społeczeństw. Intensywny rozwój sieci i systemów teleinformatycznych stymuluje rozwój nowoczesnych gałęzi przemysłu oraz nowatorskich rozwiązań w efektywnej organizacji pracy i zarządzania procesami. Z powszechnym wykorzystaniem i dynamicznym rozwojem technologii informacyjnych wiążą się, niestety zagrożenia bezpieczeństwa państw, organizacji i obywateli. Nowoczesne systemy teleinformatyczne są narażone na liczne cyberataki. Są one coraz bardziej wyrafinowane i trudniejsze do wykrycia. Celem jest zazwyczaj wykonywanie niepożądanych operacji na komputerze ofiary skutkujących m.in. dystrybucją złośliwego oprogramowania w sieci, przechwytywaniem wrażliwych informacji oraz zakłócaniem pracy.

Zespoły ds. cyberbezpieczeństwa z różnych krajów potwierdzają, że z każdym rokiem sukcesywnie wzrasta liczba incydentów i ataków w cyberprzestrzeni. W 2021 roku na podstawie 116 071 zgłoszeń zespół CERT Polska zarejestrował 29 483 unikatowe incydenty cyberbezpieczeństwa[1]. Najczęstszym typem ataku, podobnie jak w kilku ostatnich latach, były oszustwa komputerowe, które stanowiły 86,4% wszystkich obsłużonych incydentów. W stosunku do poprzedniego roku był to prawie trzykrotny wzrost. Na drugim miejscu znalazło się złośliwe oprogramowanie – 9,66% obsłużonych incydentów. Najczęściej ataki dotykały sektor mediów, handlu, poczty i usług kurierskich oraz energetyki. Zaobserwowano liczne próby wykorzystania przyzwyczajeń i nieostrożnego zachowania użytkowników sieci. Obsłużono 36 incydentów zaklasyfikowanych jako poważne, tj. takie, które mogą wpływać na świadczenie usług kluczowych. Najwięcej dotyczyło sektora bankowego.

W ostatnich latach kluczowe znaczenie ma postęp technologii mobilnych zapewniających dostęp do systemów i zasobów w dowolnym czasie i miejscu. Liczne aplikacje mobilne wspierają prowadzenie działalności gospodarczej, są stymulatorem innowacyjnych form komunikacji, prowadzą do istotnych przewartościowań w zachowaniach społecznych. Wykorzystanie elektronicznych środków komunikacji jest coraz powszechniejszą formą świadczenia pracy i kontaktów międzyludzkich. Na podstawie analiz firmy IDC[2] przewiduje się, że

1 *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2021*, Warszawa 2022.
2 https://www.idc.com/.

w Stanach Zjednoczonych w 2024 roku pracownicy mobilni będą stanowili 60% wszystkich pracowników. Nie jest zaskoczeniem gwałtownie rosnąca liczba cyberataków inicjowana przez złośliwe aplikacje mobilne lub widomości SMS.

Przeniesienie działalności do internetu oraz problemy związane z zapewnieniem bezpieczeństwa systemów komputerowych i ich użytkowników oraz niezawodnego funkcjonowania państw spowodowały podjęcie znacznych wysiłków w środowiskach nauki, administracji i biznesu. Działania te obejmują legislację, polityki i agendy dotyczące cyberbezpieczeństwa, mapy drogowe na poziomie krajowym i międzynarodowym oraz inicjowanie krajowych i międzynarodowych projektów badawczych. Wyzwaniem jest opracowanie nowych rozwiązań do skutecznej ochrony systemów komputerowych przed znanymi zagrożeniami oraz szybkiego rozpoznawania anomalii, które mogą być symptomem złośliwych działań i wykrywania nowych, nieznanych ataków. Wymaga to innowacyjnych metod i narzędzi do rozproszonego monitorowania, analizy masowych i nieustrukturyzowanych danych, klasyfikacji incydentów i wykrywania zagrożeń. Integracja danych, zaawansowane statystyki, techniki uczenia maszynowego są coraz częściej wykorzystywane do korelacji obserwowanych zdarzeń i detekcji ataków cybernetycznych.

W artykule przedstawiono przykłady potwierdzające skuteczność zastosowania metod sztucznej inteligencji do budowy systemów wykrywania złośliwego oprogramowania, konkretnie, złośliwych aplikacji mobilnych zainstalowanych na urządzeniu użytkownika. Pierwsza część pracy stanowi wprowadzenie w zagadnienia cyberbezpieczeństwa. Omawiane są popularne klasy złośliwego oprogramowania oraz metody i techniki ochrony przed atakami. Następnie uwaga koncentruje się na algorytmach uczenia maszynowego. Prezentowany jest przykład zastosowania technik sztucznej inteligencji do wykrywania złośliwych aplikacji mobilnych. Skuteczność opracowanych rozwiązań została potwierdzona przez liczne eksperymenty symulacyjne przeprowadzone na rzeczywistych danych.

Ataki komputerowe i metody obrony

Incydenty bezpieczeństwa w systemach teleinformatycznych mogą być powodowane przez zdarzenia losowe i nieumyślne działanie użytkowników lub wynikać z celowego działania osób nieuprawnionych. Ataki cybernetyczne są realizowane z wykorzystaniem różnych technik i sposobów uzyskania nieautoryzowanego dostępu do systemu komputerowego, urządzenia sieciowego,

pomiarowego czy sterującego w celu przejęcia nad nim kontroli i wydobycia informacji. W literaturze są szeroko omawiane różne wektory ataku. Ataki można klasyfikować ze względu na ich źródło, profil, cel i skutki oraz zastosowane narzędzia i techniki. Ze względu na źródło możemy wyróżnić ataki z wykorzystaniem fizycznego dostępu do urządzenia lub zdalne, wykonywane z lokalnej lub globalnej sieci. Można je przeprowadzić, wstrzykując złośliwe oprogramowanie (malicious software -- malware), wykorzystując załączniki poczty elektronicznej, specjalne strony internetowe, protokoły itd. Powstaniu sieci internet towarzyszyło pojawianie się, z czasem coraz doskonalszych i groźniejszych, odmian złośliwego oprogramowania. Różni je cel i sposób działania. Niekiedy występują łącznie, aktywując się w różnych fazach infekcji. Poniżej są wymienione przykłady najbardziej znanych klas złośliwego oprogramowania.

1. Wirus – program lub fragment kodu infekujący systemy komputerowe, dołączany do powszechnie używanych programów (nosicieli), przenoszony i powielany bez wiedzy użytkownika. Specjalna odmiana wirusa – koń trojański (tzw. trojan) – podszywa się pod użyteczne oprogramowanie i instaluje podczas pobierania programów, ściągania plików i otwierania zainfekowanych załączników.

2. Robak – samodzielny program rozprzestrzeniający się zazwyczaj za pośrednictwem sieci;

3. Exploit – program, fragment kodu lub rodzaj ataku polegający na wykorzystaniu błędów w oprogramowaniu w celu przejęcia kontroli nad komputerem użytkownika. Backdoor to celowo wprowadzona luka w systemie operacyjnym lub oprogramowaniu, która pozwala nieuprawionym osobom na obejście zabezpieczeń systemu komputerowego.

4. Ransomware – oprogramowanie blokujące dostęp do systemu lub uniemożliwiające odczytanie przechowywanych w nim danych przez założenie blokady lub zaszyfrowanie plików. Odzyskanie dostępu do systemu wymaga opłacenia okupu.

5. Spyware – oprogramowanie zbierające dane osobowe i poufne użytkownika oraz monitorujące jego aktywność, w tym przeglądane strony.

6. Keylogger – rodzaj oprogramowania śledzącego aktywność użytkownika podczas korzystania z klawiatury.

7. Rootkit – zespół programów maskujących obecność złośliwego kodu i umożliwiających włamania do systemów komputerowych.

8. Adware – oprogramowanie powodujące natrętne wyświetlanie reklam, utrudniające korzystanie z zainfekowanego urządzenia.

Celem działania złośliwego oprogramowania jest najczęściej kradzież danych, tożsamości, zasobów, zmiana ustawień sieci, instalacja fałszywych certyfikatów, deaktywacja oprogramowania zabezpieczającego przed atakami, kompromitacja wizerunku, zużycie zasobów i odmowa usługi (atak DoS – Denial of Service) itd. Często jest to zastawienie pewnej pułapki, np. fałszywej strony WWW, w celu pozyskiwania w przyszłości poufnych danych, w tym parametrów logowania do zasobów (phishing) lub przekształcenie zaatakowanego systemu w zombie (element sieci botnet), czyli przejęcie kontroli nad systemem w celu jego wykorzystania do szkodliwych działań, nieautoryzowanych przez użytkownika.

W ostatnich latach coraz częściej do przeprowadzania ataków są wykorzystywane telefony komórkowe. Ataki są inicjowane m.in. przez złośliwe aplikacje mobilne instalowane przez użytkowników i pobierane z niezaufanych źródeł lub nawet oficjalnych zasobów udostępnianych przez twórców systemów operacyjnych, np. sklep Google Play dla systemu Android. Innym sposobem są złośliwe wiadomości SMS (np. oprogramowanie Flubot) oraz e-maile zawierające linki do złośliwych aplikacji lub przekierowujące na fałszywe strony internetowe. Z badań firmy Check Point[3] wynika, że w 2021 roku 97% przedsiębiorstw miało do czynienia z atakiem na urządzenia mobilne. W 46% instytucji co najmniej jeden pracownik pobrał szkodliwą aplikację mobilną, i tym samym naraził sieć firmową na atak i ryzyko utraty informacji. Głównym źródłem ataków była sieć komputerowa. Najczęściej były to kampanie phishingowe (52%) nakłaniające użytkowników do instalacji szkodliwego oprogramowania, komunikowania się z zainfekowanym oprogramowaniem lub stronami internetowymi. Badania przeprowadzone przez firmę Check Point potwierdzają, że urządzenia mobilne są z natury podatne na ataki. Przyczyną są m.in. podatności kodu wykryte w oprogramowaniu procesorów sygnałowych firmy Qualcomm, która dostarcza układy do ponad 40% telefonów komórkowych na rynku. Wyniki prowadzonych w 2021 roku analiz prezentowane w raporcie opracowanym przez firmę Kaspersky[4] potwierdzają wykrycie 3,5 mln szkodliwych mobilnych pakietów instalacyjnych, które spowodowały 46,2 mln ataków na całym świecie i 80% tych ataków wiązało się z wykorzystaniem złośliwych aplikacji mobilnych. Wzrosła znacznie (do 2,3 mln) liczba ataków z wykorzystaniem trojanów bankowych. Eksperci firmy Kaspersky informują

3 *Mobile security report 2021*, Izrael 2022.

4 T. Shishkova, A. Kivva, *Mobile malware evolution 2021*, 21 Feb 2022, https://securelist.com/mobile-malware-evolution-2021/105876/ [dostęp: 10.01.2023].

o pojawieniu się ponad 95 tys. nowych, udoskonalonych wersji takich narzędzi. Cyberprzestępcy stawiają na jakość, koncentrują wysiłki na podnoszeniu skuteczności narzędzi ataku w celu zwiększania zysków z przestępstw komputerowych.

Powszechne stosowanie urządzeń internetu rzeczy (IoT) przyczyniło się do znacznego wzrostu zainteresowania cyberprzestępców tego typu systemami. Niezabezpieczone urządzenia pomiarowe i sterujące, tworzące systemy IoT, są wykorzystywane do prowadzenia zmasowanych ataków[5]. Najczęściej wymieniane na liście OpenWeb Application Security Project (OWASP) Top 10 Internet of Things zagrożenia to: słabe do odgadnięcia lub zakodowane hasła, niezabezpieczone usługi sieciowe, niezabezpieczony transfer i przechowywanie danych, brak aktualizacji, niewystarczająca ochrona prywatności itd. Niestety, usunięcie nawet znanych podatności jest trudne i kosztowne, gdyż często wymaga modyfikacji sprzętu i angażuje jego producenta.

Żeby sprostać dzisiejszym wymogom bezpieczeństwa i utrzymać ciągłość działania organizacji, konieczne jest zapewnienie sprawnych i skutecznych działań w celu identyfikacji i szybkiego reagowania na incydenty związane z cyberbezpieczeństwem. Systemy wykrywania włamań IDS (Intrusion Detection Systems) i systemy zapobiegania włamaniom IPS (Intrusion Prevention Systems) to części infrastruktury sieciowej wykorzystywane do ochrony sieci przed cyberatakami. Systemy IDS monitorują sieć, porównują bieżącą aktywność sieciową ze znaną bazą zagrożeń w celu wykrywania anomalii, złośliwego oprogramowania, naruszeń polityki bezpieczeństwa. Systemy IPS działają na styku sieci wewnętrznej i świata zewnętrznego. To sprzętowe lub programowe rozwiązania, których zadaniem jest uniemożliwianie przeprowadzenia ataków. Systemy IDS/IPS implementują różne architektury i metody wykrywania zagrożeń, oferują różne poziomy bezpieczeństwa[6].

Większość instytucji, zwłaszcza tych ważnych dla państwa, buduje w swoich strukturach centralne jednostki zajmujące się cyberbezpieczeństwem na

5 N. Neshenko i in., *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*, „IEEE Communications Surveys & Tutorials" 2019, t. 21, nr 3, s. 2702–2733; M. Zhuge Yu i in., *A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices*, „Future Internet" 2020, t. 12, nr 2, nr art. 27.

6 Przeglądy tego typu rozwiązań zob. m.in.: A. Khraisat i in., *Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges*, „Cybersecurity" 2019, t. 2, nr 20, s. 1–22; N. Gupta, P. Chatterjee, T. Choudhury, *Smart and Sustainable Intelligent Systems*, 2021, Wiley Online Library, DOI:10.1002/9781119752134.

poziomie organizacyjnym i technicznym (SOC – Security Operation Center). Jednostki te są wyposażane w zestawy narzędzi i usług pozwalających na monitorowanie sieci w czasie rzeczywistym i budowanie pełnego obrazu sytuacyjnego (SIEM – Security Information and Event Management). Integracja wiedzy z bezpieczeństwa informacji, procesów i technologii służących do monitorowania, analizowania i ochrony organizacji przed cyberatakami pozwala organizacjom szybko reagować na włamania i stale doskonalić procesy wykrywania i zapobiegania atakom. Tym samym systemy IDS/IPS i SIEM odpowiadają za gromadzenie, analizowanie i korelowanie danych. To zintegrowane rozwiązanie bezpieczeństwa, które łączy ciągłe monitorowanie w czasie rzeczywistym i dane z punktów końcowych z opartymi na regułach możliwościami automatycznego reagowania i analizy.

Podsumowując, zdolność do utrzymania bezpieczeństwa sieci i systemów zależy od znajomości krajobrazu zagrożeń, nowych ataków i trendów oraz podatności sprzętu i oprogramowania. Wymaga również specjalistycznych narzędzi do monitorowania globalnej sytuacji, wykrywania zdarzeń związanych z bezpieczeństwem i dostarczania danych operatorom sieci. Zespoły badawczo-rozwojowe prowadzą intensywne prace związane z zastosowaniem nowych metod, mechanizmów i technologii. W ostatnich latach obserwuje się duże zainteresowanie wykorzystaniem technik sztucznej inteligencji. Powstają nowe usługi i innowacyjne produkty umożliwiające wykrywanie i przeciwdziałanie zagrożeniom, które w znaczący sposób zwiększają bezpieczeństwo państwa, w tym ważnych instytucji i obywateli.

Metody sztucznej inteligencji w systemach wykrywania cyberataków

W literaturze dostępnych jest wiele prac prezentujących wyniki badań, których celem jest opracowanie nowych metod i narzędzi do ochrony sieci teleinformatycznych. Można wymienić wiele technik wykrywania złośliwego oprogramowania. Najważniejsze to:

1) analiza wzorców zagrożeń (sygnatur), czyli porównywanie przepływów w sieci oraz zachowań systemów i aplikacji z zestawem wcześniej utworzonych wzorców zagrożeń;

2) wykrywanie anomalii polegające na detekcji nieprawidłowych zachowań, w tym odbiegających od normy, nietypowych obciążeń sieci, specyficznych sekwencji instrukcji w kodzie aplikacji itp.

Metody wykorzystujące sygnatury pozwalają na szybką i skuteczną identyfikację złośliwego oprogramowania, ale mogą być stosowane tylko do wykrywania już znanych ataków. Wzorce są generowane na dwa sposoby, tj. tworzone manualnie lub wyznaczane automatycznie[7]. Generowanie wzorców zagrożeń wymaga eksperckiej wiedzy, jest żmudnym i skomplikowanym procesem. Do detekcji nowych zagrożeń i wykrywania anomalii stosuje się techniki eksploracji wiedzy i danych, odkrywa ukryte relacje, konstruuje różnego rodzaju heurystyki[8].

Tradycyjne podejścia do bezpieczeństwa cybernetycznego zakładające wykorzystanie baz danych o zagrożeniach oraz bazujące na doświadczeniu i wiedzy ekspertów są niewystarczające w przypadku ataków nowej generacji. W ostatnich latach coraz intensywniej do budowania modeli decyzyjnych wykorzystuje się sztuczną inteligencję (artificial intelligence – AI), a w szczególności uczenie maszynowe (machine learning – ML), które na podstawie wyszukiwania relacji w danych uczących pozwala na wydobycie istotnych informacji i wykrycie cyberzagrożenia. Najczęściej stosowanymi modelami obliczeniowymi są sztuczne sieci neuronowe (artificialneural networks – ANN) tworzone przez sztuczne neurony, imitujące w sposób uproszczony działanie ludzkiego mózgu. Obecnie dominują sieci głębokie, składające się z wielu warstw neuronów, z których każda przekształca dane wejściowe w informacje wykorzystywane przez kolejne warstwy. Mówimy wówczas o uczeniu głębokim (deep learning). Artykuł pt. „Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities"[9] zawiera przegląd publikacji z ostatnich lat poświęconych zastosowaniu AI do monitorowania sieci i wykrywania incydentów bezpieczeństwa, w tym nieprawidłowego ruchu i niebezpiecznych zachowań oraz uwierzytelniania użytkowników. Autorzy, omawiając różne podejścia, zwracają uwagę na ograniczenia i istotne wyzwania. Prezentują również autorski, koncepcyjny model cyberbezpieczeństwa. Przegląd platform obliczeniowych, w których stosuje się uczenie maszynowe do ochrony sieci

7 M. Uddin i in., *Signature-based Multi-Layer Distributed Intrusion Detection System Using Mobile Agents*, „International Journal of Network Security" 2013, nr 15, s. 97–105; P. Szynkiewicz, A. Kozakiewicz, *Design and Evaluation of a System for Network Threat Signatures Generation*, „Journal of Computational Science" 2017, t. 22, s. 187–197.

8 W. Wang, W. Wuy, *Online Detection of Network Traffic Anomalies Using Degree Distributions*, „International Journal of Communications, Network and System Sciences" 2010, nr 3, s. 177–182.

9 Z. Zhang i in., *Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities*, „Artificial Intelligence Review" 2022, t. 55, s. 1029–1053.

i systemów komputerowych, zawiera artykuł pt. „A Survey on Representation Learning Efforts in Cybersecurity Domain”[10]. Zastosowanie głębokiego uczenia do detekcji robaków sieciowych jest opisane w artykule pt. „A Worm Detection System Based on Deep Learning”[11].

Uczenie maszynowe jest również coraz częściej wykorzystywane do detekcji ataków na sieci i urządzenia mobilne. Przeglądu wybranych rozwiązań dokonano w artykule pt. „A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks”[12]. W kolejnej sekcji niniejszego artykułu jest omawiany autorski klasyfikator wykorzystujący głębokie uczenie do wykrywania złośliwych aplikacji mobilnych.

Do oceny skuteczności algorytmów detekcji cyberataków bazujących na uczeniu maszynowym wykorzystuje się różne miary. W przypadku klasyfikatora binarnego, który rozróżnia dwie sytuacje, tj. wystąpienie ataku (klasa pozytywna) oraz zachowanie normalne (klasa negatywna), wskaźniki jakości klasyfikacji są liczone na podstawie wartości macierzy błędów (confusion matrix) zawierającej wyniki klasyfikacji. Są to cztery wartości: TP (True Positive) – liczba rzeczywistych ataków zaklasyfikowanych do klasy pozytywnej (poprawnie) i FN (False Negative) zaklasyfikowanych do klasy negatywnej (niepoprawnie) oraz TN (True Negative) – liczba wyników świadczących o normalnym stanie systemu zaklasyfikowanych do klasy negatywnej (poprawnie) i FP (False Positive) zaklasyfikowanych do klasy pozytywnej (niepoprawnie). Poniżej prezentowane są trzy główne miary do oceny jakości klasyfikacji.

1. Dokładność (accuracy) – określa prawdopodobieństwo poprawnej klasyfikacji

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}. \tag{1}$$

2. Precyzja – pokazuje jaka część wyników sklasyfikowanych jako pozytywne należy faktycznie do klasy pozytywnej

$$Precision = \frac{TP}{TP + FP}. \tag{2}$$

10 M. Usman i in., *A Survey on Representation Learning Efforts in Cybersecurity Domain*, „ACM Computing Surveys” 2019, t. 52, s. 1–28.

11 H. Zhou i in., *A Worm Detection System Based on Deep Learning*, „IEEE Access” 2020, t. 8, s. 205444–205454.

12 E. Rodríguez i in., *A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks*, „IEEE Communications Surveys &Tutorials” 2021, t. 23, nr 3, s. 1920–1955.

3. Czułość – określa zdolność klasyfikatora do wykrywania klasy pozytywnej

$$Sensitivity = \frac{TP}{TP + FN}. \quad (3)$$

Przykład zastosowania sztucznych sieci neuronowych do wykrywania złośliwych aplikacji mobilnych

System Android jest obecnie dominującym systemem operacyjnym dla urządzeń mobilnych. Korzysta on z aplikacji, które są zazwyczaj dystrybuowane jako pliki APK (Android Package Kit). Jest to skompresowane archiwum składników danej aplikacji. Podstawowymi elementami APK są: 1) plik AndroidManifest.xml zawierający informacje o aplikacji, w tym charakterystyczne atrybuty, 2) plik classes.dex zawierający m.in. skompilowany kod aplikacji. Decyzja o tym, czy dana aplikacja jest złośliwa jest najczęściej podejmowana na podstawie aktualnej zawartości jednego lub obu wymienionych plików[13].

Zaprojektowany i wykonany autorski system wykrywania złośliwych aplikacji mobilnych na urządzeniach pracujących pod kontrolą systemu Android stosuje analizę statyczną kodu zawartego w pliku classes.dex. Na potrzeby detekcji cyberzagrożeń zbudowano dwa klasyfikatory – dwa modele złożonych sztucznych sieci neuronowych:

1) CNN – splotowa sieć neuronowa;
2) RCNN – rekurencyjna sieć neuronowa z warstwami splotowymi[14].

Do uczenia i testowania sieci wykorzystano 3339 odpowiednio przetworzonych próbek aplikacji szkodliwych pobranych z repozytorium próbek złośliwego oprogramowania VirusShare[15] oraz 3390 próbek aplikacji nieszkodliwych z witryny F-Droid[16]. Podział zbioru był następujący: zbiór uczący – 80% próbek, zbiory walidujący i testowy – po 10% próbek. Obie sieci zostały wytrenowane na zbiorze uczącym. Modele, dla których uzyskano najlepsze wyniki detekcji dla zbioru walidacyjnego, zostały wybrane do eksperymentów

13 S. Arshad, A. Khan, A. Mansoor, M. Shah, *Android Malware Detection and Protection: A Survey*, „International Journal of Advanced Computer Science and Applications" 2016, t. 7, nr 2, s. 342–351; Z. Ren i in., *End-to-End Malware Detection for Android IoT Devices Using Deep Learning*, „Ad Hoc Networks" 2020, t. 101, s. 102098.
14 Ch.C. Aggarwal, *Neural Networks and Deep Learning*, Cham 2018.
15 https://virusshare.com/.
16 https://www.f-droid.org/.

mających na celu sprawdzenie skuteczności klasyfikatorów. Wykonano po kilkanaście eksperymentów dla każdej sieci. Wykorzystano do tego celu zbiór testowy złożony z próbek złośliwych i niezłośliwych. Uśrednione i najlepsze wartości miar zdefiniowanych formułami (1)–(3) prezentuje tabela 1.

Tabela 1. Porównanie skuteczności dwóch modeli klasyfikatorów na przykładzie dziesięciu eksperymentów

Model sieci	Średnie wartości miar [%]			Wartości miar dla modeli o najwyższej uzyskanej dokładności [%]		
	Acc	Precision	Sensitivity	Acc	Precision	Sensitivity
CNN	84,94	88,97	79,70	86,57	88,61	83,83
RCNN	87,96	91,54	83,35	93,28	93,92	92,51

Źródło: R. Litka, *Detekcja złośliwych aplikacji na urządzenia mobilne z wykorzystaniem uczenia maszynowego*, Warszawa 2021.

Wyniki testów potwierdzają wysoką skuteczność opracowanych narzędzi do wykrywania złośliwych aplikacji mobilnych. Pokazują także dość istotną przewagę klasyfikatora, w którym dodano warstwy rekurencyjne. Rozbudowa struktury sieci skutkuje, oczywiście większą złożonością obliczeniową. Czas uczenia sieci RCNN był około cztery razy dłuższy niż sieci CNN. Niemniej jednak ponad 5-procentowe zwiększenie dokładności klasyfikacji danych może istotnie wpłynąć na dokładność wykrywania ataków.

Zakończenie

Większość powszechnie używanych urządzeń takich jak smartfony, ale również tablety, laptopy itp. pracuje pod kontrolą systemu Android. Stąd ważne jest zapewnienie bezpieczeństwa i ochrona przed cyberatakami tego systemu oraz aplikacji działających pod jego kontrolą. Prezentowany przykład zastosowania dwóch modeli klasyfikatorów wykorzystujących głębokie uczenie do wykrywania złośliwych aplikacji na urządzenia mobilne potwierdza, że narzędzia informatyczne wykorzystujące metody sztucznej inteligencji mogą znacząco wspierać zespoły zajmujące się cyberbezpieczeństwem. Należy podkreślić, że opracowane i wykonane klasyfikatory mogą pracować w pełni autonomicznie, a przeprowadzone dodatkowe eksperymenty potwierdzają, że ich skuteczność rośnie wraz ze wzrostem wolumenu danych uczących. Koszt obliczeniowy nie jest duży, uczenie przebiega szybko, więc może być realizowane na urządzeniu o niewielkich zasobach, jakim jest np. telefon komórkowy.

Bibliografia

Aggarwal Ch.C., *Neural Networks and Deep Learning*, Cham 2018.

Arshad S., Khan A., Mansoor A., Shah M., *Android Malware Detection and Protection: A Survey*, „International Journal of Advanced Computer Science and Applications" 2016, t. 7, nr 2.

Gupta N., Chatterjee P., Choudhury T., *Smart and Sustainable Intelligent Systems*, 2021, Scrivener Publishing LLC, Wiley Online Library.

Khraisat A. i in., *Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges*, „Cybersecurity" 2019, t. 2, nr 20.

Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2021, Warszawa 2022.

Litka R., *Detekcja złośliwych aplikacji na urządzenia mobilne z wykorzystaniem uczenia maszynowego*, Warszawa 2021.

Mobile security report 2021, Izrael 2022.

Neshenko N. i in., *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations*, „IEEE Communications Surveys & Tutorials" 2019, t. 21, nr 3.

Ren Z. i in., *End-to-End Malware Detection for Android IoT Devices Using Deep Learning*, „Ad Hoc Networks" 2020, t. 101.

Rodríguez E. i in., *A Survey of Deep Learning Techniques for Cybersecurity in Mobile Networks*, „IEEE Communications Surveys & Tutorials" 2021, t. 23, nr 3.

Shishkova T., Kivva A., *Mobile malware evolution 2021*, 21 Feb 2022, https://securelist.com/mobile-malware-evolution-2021/105876/ [dostęp: 10.01.2023].

Szynkiewicz P., Kozakiewicz A., *Design and Evaluation of a System for Network Threat Signatures Generation*, „Journal of Computational Science" 2017, t. 22.

Uddin M. i in., *Signature-based Multi-Layer Distributed Intrusion Detection System Using Mobile Agents*, „International Journal of Network Security" 2013, nr 15, s. 97–105.

Usman M. i in., *A Survey on Representation Learning Efforts in Cybersecurity Domain*, „ACM Computing Surveys" 2019, t. 52.

Wang W., Wuy W., *Online Detection of Network Traffic Anomalies Using Degree Distributions*, „International Journal of Communications, Network and System Sciences" 2010, nr 3, s. 177–182.

Zhang Z. i in., *Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities*, „Artificial Intelligence Review" 2022, t. 55.

Zhou H. i in., *A Worm Detection System Based on Deep Learning*, „IEEE Access" 2020, t. 8.

Zhuge Yu M. i in., *A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices*, „Future Internet" 2020, t. *12*, *nr 2*.

Attacks on mobile devices and methods of detection

Abstract

Individual protection of autonomous systems using simple analysis of transmitted messages is unfortunately becoming insufficient. There is a clear need for new solutions using data from multiple sources, integrating various methods, mechanisms and algorithms, including Big Data processing and data classification techniques using artificial intelligence methods. The quantity, quality, reliability and timeliness of data and information about the network situation, as well as the speed of its processing, determine the effectiveness of protection. The paper presents examples of the application of various artificial intelligence techniques for detecting attacks on ICT systems. Attention is focused on the application of deep learning methods for the detection of malicious

applications installed on mobile devices. The effectiveness of the presented solutions was confirmed by numerous simulation experiments conducted on real data. Promising results were obtained.

Key words: cybersecurity, cyberattack detection, mobile applications, artificial intelligence, machine learning, artificial neural networks, deep learning

Piotr Milik*
Grzegorz Pilarski**

Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system – theory and practice

Abstract

The article discusses the matter of contemporary cyberattack techniques aimed at the financial security of banks and their clients and presents the relationship of banks with their clients in the light of the applicable provisions of the European Union (Directive of the European Parliament and the EU Council 2015/2366 of November 25, 2015 on payment services in internal market) and the Polish Act of 19 August 2011 on payment services. The authors also analyze the practical side of the relationship between banks and their customers who have fallen victim to computer fraud, pointing out that the common practice of banks refusing to return funds stolen from their customers in the electronic banking system is inconsistent with the applicable standards of Polish and European law.

Key words: cyberattack, financial security, electronic banking system, computer fraud, European Union

* Assoc. Prof. Piotr Milik, PhD, War Studies University in Warsaw, e-mail: p.milik@akademia.mil.pl, ORCID: 0000-0002-1204-4882.
** Assoc. Prof. Grzegorz Pilarski, PhD, War Studies University in Warsaw, e-mail: g.pilarski@akademia.mil.pl, ORCID: 0000-0001-9728-2611.

Introduction

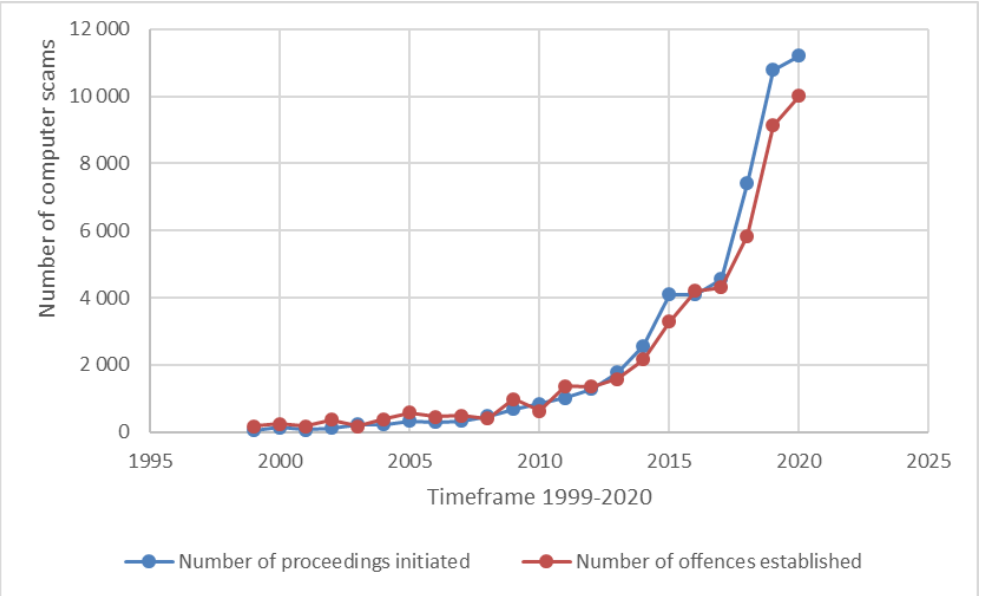
Internet banking dates back to the beginning of the 1990s. It was started in the United States of America, where the first transactions in cyberspace were carried out via the still fledgling Internet. Nowadays, all financial institutions, including banks, provide their clients with special systems, thanks to which they can perform financial operations without leaving home, only with the use of a home computer or personal smartphone.

Today's cyberspace is a global network consisting of interconnected ICT systems built of devices that enable the creation, processing and exchange the information automatically between devices or consciously and intentionally between their users. Cyberspace defined in this way (constituting a zone of everyday activity of states and their citizens, in which the interests of these entities are pursued) is constantly threatened in the first place by illegal activities of persons and criminal groups, including terrorist groups, and then also as a result of errors or failure of individual ICT systems.

The COVID-19 pandemic that the world collided with in 2020 has accelerated the computerization of public and private services. The information (digital) revolution that we have witnessed in recent decades has accelerated. The life and professional activity of developed societies has largely moved to cyberspace. Common education, academic lectures, banking operations, purchases of all kinds of goods and services, communication with public institutions almost overnight moved to the Internet. Developed societies have undergone an accelerated course in the use of new information technologies. Unfortunately, the rapid pace of these changes resulted in an intensified wave of abuse. Cybercrime has flourished as digital online operations intensify. The issue of cybersecurity has become more important and topical than ever before.

The Scale of Unauthorized Payment Transactions

The years of the COVID-19 pandemic, in addition to technological development and the growing role of the Internet in modern society, contributed to the increase in committing computer frauds enshrined in Art. 287 of the Polish Criminal Code. Figure 1 below presents statistical data relating to this type of crime.



Source: own study based on data from the website https://statystyka.policja.pl [access: 15.10.2022].

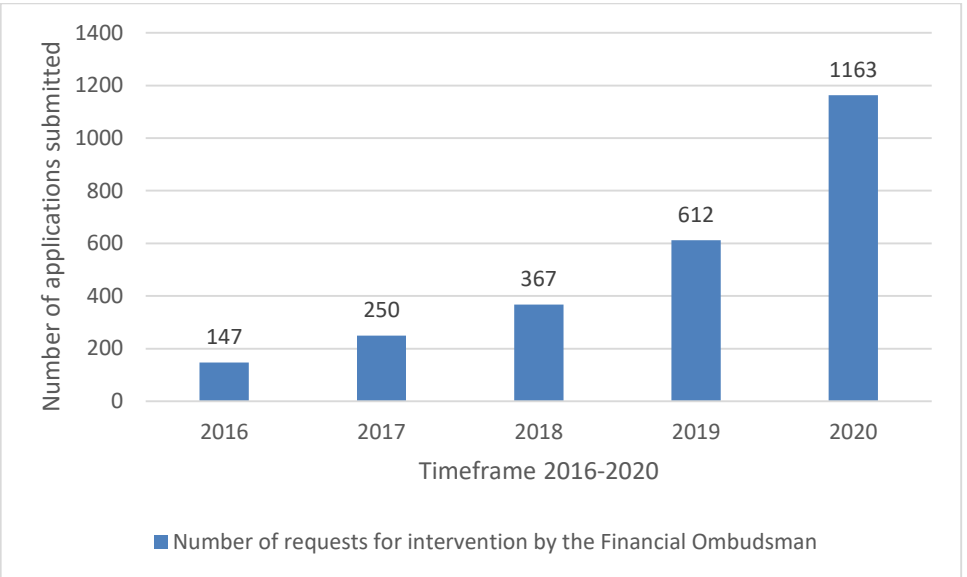
Figure 1. The number of computer frauds under art. 287 CC in the years 1999–2020

Based on the above data, it can be clearly stated that the number of computer frauds has almost doubled since 2019. These crimes relate to various spheres of the functioning of society. One of them is finance, which can be seen from the increase in unauthorized payment transactions over the past few years. This type of transaction is not defined by law, however, pursuant to the PSD2 directive[1], Art. 64 (sec. 1), an authorized transaction is considered a payment transaction only if the payer grants consent to execute this payment transaction (the transaction authorization may be performed before or after the execution of the payment transaction), and in the event of disagreement, the payment transaction is considered as unauthorized (sec. 2). Moreover, in Art. 74 (sec. 3) there is a provision stating that „the payer shall not bear any financial consequences resulting from the use of a lost, stolen or misappropriated payment instrument, unless he acted with dishonest intentions". The condition for such a state to occur is notification by the payer

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC, Official Journal of the European Union 2015, L 337/35.

in accordance with Art. 69 (sec. 1b) of the loss, theft, misappropriation or unauthorized use of a payment instrument. The guidelines of the European Banking Authority (EBA) indicate that an unauthorized transaction is one that was performed without the consent of the payer. In this case, the payment instrument can be either a credit card or a banking application enabling access to a bank account. These provisions show that an unauthorized transaction may also be an authenticated transaction, but made without the consent of the payer.

Based on the data posted on the Polish Financial Ombudsman's website, an upward trend of this phenomenon can be observed in the form of the number of submitted applications for the intervention of the Financial Ombudsman, which is illustrated in Figure 2.



Source: own study based on data from the website https://rf.gov.pl [access: 15.10.2022].

Figure 2. Number of submitted applications for the intervention of the financial ombudsman in disputes regarding unauthorized transactions in 2016–2020

Quantitative data clearly indicate an upward trend in the problem of unauthorized transactions on the financial market. This is related to two main points. The first relates to committing computer crimes related to the making of unauthorized financial transactions, and the second to the actions of banks in this regard, i.e. not reimbursing clients for losses incurred despite the existence of such a statutory obligation. Banks indicate the provisions

of the Payment Services Act as the basis for the refusal, where in Art. 46 indicates the fault of the payer of an unauthorized payment transaction as a result of intentional or grossly negligent breach of his obligations. According to experts, as a result of the development of e-services such as e-commerce[2], m-banking[3], e-banking[4], and open banking[5], one should expect an increase in computer fraud in the form of unauthorized payment transactions.

Threats of an Unauthorized Payment Transaction

In this part of the article, the authors present examples of threats for the payer that may result in an unauthorized transaction. Payment fraud can occur in the transaction system as a result of threats such as[6]: 1) social engineering and phishing activities; 2) malicious programs (malware); 3) APT (Advance Persistent Treats); 4) denial of access DDoS (Denial Distribution of Service); 5) botnets; 6) other threats.

In terms of payment crimes, the above threats may affect specific transaction processes[7], which is presented in the table below (Table 1).

You should be aware that this is only a demonstrative assignment of threats that may arise with high probability in the implementation of specific transaction operations. The first group of threats concerns the attack vector directed not at the technologies used, but at the human who uses them. Social engineering are specific activities that use human error to achieve the intended benefits. In the field of social engineering, attackers use various techniques to try to influence the opinion of the attacked person and make them disclose, for example, confidential information.

2 E-commerce – electronic commerce, a type of commerce that enables the conclusion of commercial transactions using the Internet.

3 M-banking – a financial service enabling access to a payment instrument via mobile devices with Internet access.

4 E-banking – a financial service enabling access to a payment instrument through: computer, ATM, POS terminal, mobile phone, telecommunications line and the Internet. This service enables the implementation of transactional banking.

5 Open banking – a new standard of payment services, in which financial service providers are required to provide third parties with the so-called TPP (Third Party Providers) access to payers' accounts through the so-called API (Application Programming Interface) in accordance with the EU directive PSD2.

6 *2021 Payment Threats and Fraud Trends Report*, Brussels 2021, p. 3.

7 Ibidem, p. 19.

Table 1. Impact of financial payment threats on transaction-related processes

Selected transaction processes	Social engineering	Malware	APT	DDoS
On-boarding/ Provisioning	X	X		
Invoicing/payment request	X	X		
Initialization/ Authentication	X	X		
Payment processing	X	X	X	X

Source: *2021 Payment Threats and Fraud Trends Report*..., p. 19.

In terms of techniques used for the needs of a social engineering attack, the following activities can be distinguished: 1) online baiting – a form of a social engineering attack consisting in „luring" a potential victim through a properly prepared online advertisement that contains a link to initiate the installation of malware in the operating system; an example may be encouraging to take advantage of the opportunity to open a favorable term deposit with a high interest rate well above what the banks actually guarantee on the market; 2) phishing – a social engineering technique consisting in sending messages using e-mail containing content encouraging to click on a link included in the message; an example may be a message from a bank describing that the user's account has been compromised by breaking the password and in order to confirm this situation, it is recommended to log into the account via a link included in the message, which directs to a crafted bank's website that is confusingly similar to the real page, in order to obtain authentication data i.e. login and password; attacks of this type can be divided into spear phishing, whaling and CEO fraud – these are personalized attacks that also impersonate employees of the organization in which the victim works, including e.g. the CEO (General Manager); 3) vishing and smishing – these are social engineering techniques that are used respectively by an initiated telephone conversation or a properly prepared SMS; an example message and conversation may concern a situation in which the bank or a person from the bank provides information that the payer's account will be deactivated and to avoid this, log in to your account via a link (referral to a fake bank's website) or provide login details; 4) online enticement – a technique that uses advertisements on the Internet, which are characterized by the fact that they offer too favorable conditions than it could be in reality, e.g. a reduction in the

purchase of computer equipment at the level of 80% of the market price or a false offer of „click credit", etc.; 5) romance scam – in this technique we deal with a criminal assuming a false internet identity in order to gain the trust and sympathy of a potential victim of fraud, manipulation or robbery of the victim. This is possible by creating the illusion of a close relationship; in 2021, social engineering attacks using this technique were among the most financially harmful cyberattacks[8]; 6) spoofing – a social engineering attack technique in which the attacker impersonates an organization or financial entity, creates a counterfeit domain of a real company to provide WWW and e-mail services that are used to obtain the payer's confidential data; 7) pretexting – this is a technique that enables the preparation of an appropriate social engineering attack and consists in creating a context in the form of a hypothetical story, which is used by an employee of e.g. a bank to obtain confidential information, forging is carried out usually by phone call.

The second group of threats concerns the use of malicious programs (malware). It is assumed that any type of malware is designed to harm an IT system or steal data[9]. The use of malware is one of the biggest threats to cybersecurity today. This type of threat is currently used for a wide range of activities, in which we can distinguish among others: gaining remote access to information systems; damage or deactivation of computers or information systems; spying, modifying, damaging or intercepting data without the user's consent[10]. These and other malicious actions are possible to implement thanks to various types of malicious programs, which include: viruses, worms, trojans, exploits, etc. In terms of the occurrence of unauthorized payment transactions, one of the most dangerous and effective actions can be carried out using trojans. A software called a trojan horse, a trojan is a type of software disguising itself as useful or interesting applications that, when launched by the user, may allow criminals to perform undesirable activities such as: spying

8 *FBI: 6,9 miliarda dolarów – tyle w 2021 roku utracono z powodu przestępstw internetowych*, CyberDefence24, Warszawa 2022, https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-69-miliarda-dolarow-tyle-w-2021-roku-utracono-z-powodu-przestepstw-internetowych [access: 5.09.2022].

9 J. Janczak, G. Pilarski, B. Biernacik, *Technologia informacyjna w zarządzaniu*, Warszawa 2009, p. 171.

10 J. Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015, p. 93.

and stealing confidential user data (spyware[11]); installing backdoor software[12] that allows access to the system bypassing security measures, for example, to send spam or carry out DDoS attacks; deletion, modification and encryption of data, e.g. ransomware[13].

Another group of threats concerns APT (Advanced Persistent Threat) attacks, which means:

– Advanced – attackers use various techniques and methods to effectively breach security, use known vulnerabilities and also look for new vulnerabilities to carry out a given attack;

– Persistent (prolonged, persistent, stubborn) – the attack is to be effective, performed in such a way that it does not attract anyone's attention, and after gaining access to one victim's system, the purpose of the attack is to extend the control to other systems in a way that allows long-term and constant presence and supervision;

– Threat – because the attacker is an organized group with the appropriate technical background and budget. The threat remains constant as long as the attacker has the (political, economic) incentive to steal the victim's information[14].

These types of attacks can target a specific person, company, organization, institution or state. Attackers use highly personalized tools (exploits, viruses, worms, rootkits, zero-day vulnerabilities) and hacking techniques often developed for a specific attack. Attacks of this type may be directed at financial institutions in order to hack into payment networks or systems with the intention, for example, to execute unauthorized payment transactions and steal means of payment.

The next group of threats concerns DDoS access denial attacks and the use of botnets. DDoS is a tool used to damage or prevent the correct operation of the victim's ICT infrastructure. These activities may contribute to the loss of reputation of financial institutions or hinder customer service. DDoS attacks are performed by many, sometimes hundreds of thousands

11 Spyware – designed to collect information about the user, as well as send it to third parties without the user's knowledge.

12 Backdoor – A security or software vulnerability created intentionally by the software developer that could allow access to the user's operating system bypassing security systems.

13 Ransomware – a type of malware that can steal and encrypt user data in order to obtain a ransom for unlocking data or not disclosing it.

14 See G. Pilarski, *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020, p. 69–73.

of devices connected to each other in the so-called botnet network. Botnets are a collection of devices connected to the Internet that were previously attacked by criminals in order to take control over them without the victim's knowledge. The purpose of these attacks is to enable DDoS, spam or ransomware campaigns. In recent years, this type of activity has become more and more popular among cybercriminals, an example of which is the Emotet botnet, which in 2021 contributed to malware infection of 19% of companies around the world[15].

Other threats that may constitute transaction frauds include all kinds of activities aimed at obtaining data enabling the use of e-banking services, in particular the use of payment instruments in the form of credit and debit cards. In order to obtain data enabling the execution of electronic transactions, criminals use various methods, including: 1) installation of additional illegal devices in ATMs: card reader (skimming – enables reading data from the magnetic stripe of the card); keyboard overlays (fake keyboard – allows you to register PIN codes entered for cards); hidden cameras (hidden cameras – allow you to record the payment process, which allows you to obtain a PIN, card number and CVV/CVC codes); card trapping mechanism – allows the card to be retained when it is introduced to an ATM in order to obtain it after the payer leaves, false fronts (placed on ATMs in order to obtain credentials); 2) the use of public wi-fi networks and fake applications – using these tools, cybercriminals can collect confidential user data, including data enabling authentication in transaction systems; 3) use of false documents – fraudsters using stolen personal data, obtained from forms, applications, etc., that have been lost, stolen or thrown away, produce new cards or other payment instruments that enable payment transactions to be made without the payer's knowledge.

The authors are aware that the above catalog of threats is not a complete catalog and presents selected examples, moreover, it should be taken into account that new methods and techniques are emerging that are used by criminals in the field of payment fraud, which may lead to unauthorized payment transactions.

15 M. Duszczyk, *Powraca najbardziej niszczycielski cyberwirus. Firmy mają powody do obaw*, „Rzeczpospolita", 23.11.2021, https://firma.rp.pl/biznes/art19126551-powraca-najbardziej-niszczycielski-cyberwirus-firmy-maja-powody-do-obaw-emotet-cyberwirus_IT [access: 10.09.2022].

One of the most important measures to be applied in the field of payment fraud prevention is increasing security awareness among various stakeholders in the payment system.

Examples of initiatives in this area were presented by the Polish Financial Ombudsman (FO) in his report on unauthorized payment transactions[16], where he described the procedure to be followed after identifying irregularities by the payer. According to FO, the following actions should be taken:

1. After discovering a transaction fraud, you should immediately notify: your bank, the CERT.PL team (incydent.cert.pl), the nearest police unit (reporting and obtaining a certificate of committing a crime).

2. Filing a financial claim with your bank for the reimbursement of lost funds.

3. If the bank does not respond within D + 1, a complaint should be submitted, which should be processed within 15 working days.

4. If the bank proves that: a) the transaction was made by an authenticated person trying to defraud the bank, b) the payer breached its obligations intentionally or as a result of gross negligence[17], c) the payer will be required to return previously declared financial claims.

5. In the event of a dispute with a bank, an application for intervention may be submitted to the Financial Ombudsman or the Consumer Ombudsman.

In terms of recommendations addressed to both the payment service provider and the payer, an important element of security are guidelines and recommendations developed by the Polish Financial Supervision Authority[18].

16 *Nieautoryzowane transakcje – zasady i główne problemy*, Warszawa, 18 czerwca 2019, p. 13, https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf [access: 5.09.2022].

17 Pursuant to Art. 42 of the Act on Payment Services, the obligations of the payer include: using the payment instrument in accordance with the principles set out in the contract; promptly reporting the loss, theft, misappropriation or unauthorized use of a payment instrument or unauthorized access to it; taking the necessary measures to prevent the violation of individual security features of this instrument, in particular, is obliged to store the payment instrument with due diligence and not to disclose it to unauthorized persons.

18 Interesting documents in this regard include: *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, Warszawa 2015, https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf [access: 12.08.2022]; *Rekomendacje dotyczące bezpieczeństwa płatności internetowych*, Frankfurt n. Menem 2013; *Ostrzeżenie przed dopuszczaniem pośredników do rachunku bankowego w płatnościach internetowych*, Warszawa 2016, https://www.knf.gov.pl/knf/pl/komponenty/img/ostrzezenie_posrednicy_platnosci_60551.pdf [access: 10.09.2022]; K. Leżoń, *Otwarta bankowość w świetle wymogów*

The role of the payer in increasing the level of security of payment transactions is, first of all, to properly ensure the security of the payment instrument and to use the latest solutions and technologies recommended by the payment service provider of the transaction system. One of the user's actions is taking care not to provide access to data that enables authentication (login and password); use of strong passwords with a minimum length of more than 15 characters; use of two-factor authentication mechanisms; reporting irregularities in payment services to relevant authorities; use of payment solutions without the need to use payment cards (non-cash payments, withdrawals and deposits at ATMs).

Banks' Reactions to Unauthorized Payment Transactions

Under Polish law, the basic document defining the rules for the provision of payment services, as well as the scope of the providers' liability for the performance of payment services, is the Act of August 19, 2011 on payment services (consolidated text, Journal of Laws 2019, item 659) – Payment Services Act.

The solutions included in the Payment Services Act were aimed at standardizing the method of providing payment services and regulating the activity of providing payment services in such a way as to ensure the harmonization of the provision of these services throughout the European Union. The Act implemented Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market and amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (PSD directive), which is the so-called directive full harmonization.

The new Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) No 1093/2010 and repealing Directive 2007/64/EC.

In the above-mentioned, current EU directive we can read (rule 71) that in the case of an unauthorized payment transaction, the payment service provider should immediately return the amount of this transaction to the payer,

dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech, Warszawa 2019.

unless there is a high probability of an unauthorized transaction resulting from fraudulent actions of the payment service user and this suspicion based on the objective grounds notified to the relevant national authority. In this case, the payment service provider should carry out an investigation within a reasonable period of time before making a refund to the payer. In order to encourage the payment service user to report to his payment service provider without undue delay on any theft or loss of the payment instrument, and thus to reduce the risk of unauthorized payment transactions, the user should only be liable up to a very limited amount, unless that user has acted fraudulently intentions or has been guilty of gross negligence in doing so. In this context, an amount of EUR 50 appears to be adequate to ensure a harmonized and high level of user protection in the European Union. The payer should not be held liable if he or she could not have been aware of the loss, theft or misappropriation of the payment instrument. Moreover, from the moment the user reports to the payment service provider that there may have been an unauthorized use of his payment instrument, the payment service user should not be required to bear any further losses resulting from the unauthorized use of that instrument. The aforementioned provision of the EU Directive establishes a general principle of the liability of a bank (payment service provider) for unauthorized payment transactions. In such a situation, the bank should immediately return the amount of this transaction to the payer (bank customer). In other words, the European legislator formulates a postulate that the money credited to the client's bank account belongs to the bank and not to the client, and therefore the potential theft of funds from the client's account is actually detrimental to the bank. An exception has been formulated from this rule, concerning a situation where a bank's client acts knowingly to the detriment of the bank or commits gross negligence in using a payment card or access codes to an internet account.

The above-mentioned principles are implemented into Polish law by the above-mentioned Act of 19 August 2011 on payment services (Payment Services Act).

Unfortunately, despite the clear and precise provisions of the EU Directive and the Polish Payment Services Act, banks, as providers of electronic services, do not comply with their provisions. Banks, after receiving a complaint from their client indicating the occurrence of an unauthorized payment operation (theft of funds over the Internet from the client's bank account), each time refuse to return the stolen money to the client's account. A negative response to the complaint is a standard among financial institutions in Poland. In

response to the complaints, the banks refer to Art. 46 sec. 3 of the Act of 19 August 2011 on Payment Services, which states that „The Payer is responsible for the full amount of unauthorized payment transactions if he caused them intentionally or as a result of intentional or grossly negligent breach of at least one of the obligations referred to in Art. 42". At the same time, they indicate that the customer's behavior, such as clicking on a link pointing to a fake bank website and providing authorization data there, is a grossly negligent act.

In the situation described above, there are several scenarios of the bank's customer behavior and several possible reactions from the bank itself.

Firstly, customers let go of the further battle with the bank after receiving a negative response to the complaint. Then the illegal behavior of the bank has no consequences for it. Despite the lack of detailed data, it can be assumed that this is the case of the vast majority of reactions from bank customers who do not believe in effective pursuit of their claims against the bank, and do not know the applicable law in this regard.

Secondly, some bank customers attempt to act independently and submit a complaint to the Polish Financial Ombudsman, acting pursuant to the Act of 5 August 2015 on Complaints Handling by Financial Market Entities and on the Financial Ombudsman. This extends the entire client's recovery process and does not have the direct effect of returning stolen funds to the client. The ombudsman may, at best, issue an opinion favorable to the client on the matter, which may be brought before the court, if the client decides to sue the financial institution.

Thirdly, as it seems, the least numerous group of defrauded bank customers report to a professional representative – an attorney or legal advisor, requesting legal assistance immediately after the theft. This is undoubtedly the most effective method of pursuing claims against banks, because professional representatives are perfectly familiar with the applicable regulations and procedures and can effectively enter into relationships with banks on behalf of defrauded clients.

Professional representatives send requests for payment to the banks, in which they ask banks to fulfill their statutory obligations and return the money stolen from their online accounts to customers, informing at the same time that in the absence of a positive reaction, the case will be referred to a common court. In such a situation, banks proceed three ways to behave. First, immediately upon receipt of a payment order signed by a professional representative, they return the stolen money to the customers in full. Such

a situation takes place when the stolen sums are not too large, it can be assumed that they reach several thousand złotych.

In the case of higher amounts, the banks address the client directly, bypassing the professional representative, with a proposal to conclude a settlement in which the bank undertakes to return the entire sum of money stolen from the client, and the client undertakes not to disclose the content of the settlement to third parties, including his professional representatives. In the indicated situation, the customer will receive a cash refund, but will not be able to publicly inform about it, e.g. via social media, under the penalty of canceling the settlement and taking the money back. The bank returns the stolen money and gains a guarantee that the rest of its current and potential customers, including deceived customers, will not find out that such a procedure exists, thus the bank will be able to continue to refuse to return money to customers robbed via the Internet with impunity.

Finally, there is also a way for banks to delay and wait for the client to successfully file a lawsuit, which involves the client's costs of legal representation and other costs of the trial, including a court fee in the amount of 5% of the value of the dispute (stolen money). For some clients, court costs may constitute a significant barrier in deciding to engage in a court battle, the outcome of which no one can guarantee to the client. However, even when the lawsuit is successfully filed, the bank may conclude a settlement with the client and agree to return the stolen money without waiting for a court judgment unfavorable to the bank.

Statement of the Financial Ombudsman

Pursuant to the interpretation of the provisions of the Act of 19 August 2011 on Payment Services, consistently presented by the Polish Financial Ombudsman, banks should, pursuant to Art. 46 sec. 1 of the cited act, first return their clients money they lost as a result of unauthorized transactions, and only then, if they claim that there has been gross negligence on the part of their clients, to demand the return of the funds paid out in court. Then the burden of proof and the costs of initiating court proceedings rest with the banks initiating the proceedings, and the court decides about the actual gross negligence of their clients.

In the opinion of the Polish Financial Ombudsman, as a result of the implementation of the PSD2 directive, Art. 46 of the Payment Services Act,

results in significant changes to the procedure to be followed in the case of unauthorized payment transactions. Until 20 June 2018, in the event of an unauthorized payment transaction, the payer's provider was obliged to immediately return the amount of the unauthorized payment transaction to the payer, and, if the payer uses the payment account, restore the debited payment account to the state that would exist if the unauthorized transaction had not taken place. According to the new wording of Art. 46 sec. 1 of the cited act, in the event of an unauthorized payment transaction, the payer's supplier shall promptly, but not later than by the end of the business day following the day when the unauthorized transaction has been debited from the payer's account has occurred, or after receiving the relevant notification, returns the amount of the unauthorized payment transaction to the payer – with except when the payer's supplier has reasonable and duly documented grounds to suspect fraud and informs the law enforcement authorities of this in writing. Where the payer is using the payment account, the payer's provider shall restore the debited payment account to the state that would have existed if the unauthorized payment transaction not taken place. In the opinion of the Financial Ombudsman, this change is of paramount importance for the procedure to be followed in the event of an unauthorized payment transaction. In the opinion of the Financial Ombudsman, according to the current legal status, in the event of an unauthorized transaction, there are several basic rules. Rule 1: obligation to return funds to the client unconditionally; rule 2: obligation to refund the amount of the unauthorized transaction by D + 1; rule 3: establishing the rules of the payer's possible liability for an unauthorized transaction only after the funds have been returned.

From the provision of Art. 46 sec. 1 of the Payment Services Act, after the amendment, it results primarily that the national legislator, following the EU legislator, introduced the obligation to unconditionally return the amount of an unauthorized transaction to the payer by supplier.

The supplier should refund the amount of the unauthorized transaction immediately, and at the latest on the next business day after the notification or detection of unauthorized transaction. As we can see, the EU legislator decided to introduce very short deadline for the supplier to return the amount of the unauthorized transaction payment, while imposing on him an obligation to adopt such internal procedures that will allow him to be carried out within a reasonable time investigating whether there has been any fraudulent activity in a given case the payment service user himself.

In the opinion of the Financial Ombudsman, there is a rule, unconditional obligation to return funds from an unauthorized payment transaction by the provider, as soon as it is detected or found, and only after this return has been made the principles of possible joint liability of the payer for an unauthorized payment transaction. Establishing this joint liability is related to the factual and legal assessment of certain events, hence, in the opinion of the Financial Ombudsman, it should take place in the course of court proceedings.

In the opinion of the Financial Ombudsman, there are only two exceptions to the unconditional rule to return the funds to the customer. First, the documented suspicion of fraud and notification of law enforcement agencies. Secondly, the client's failure to meet the deadline reporting of an unauthorized transaction.

At this point, it should be noted that the evaluation of evidence in the Polish legal system has been assigned to common courts, hence payment service providers who are interested in a positive outcome for them in accordance with the principle „Nemo iudex in causa sua" cannot be judges in their own case[19].

Bank Account Agreement as an Irregular Deposit

In addition, it should be noted that the customer and the bank are bound by a bank account agreement. Pursuant to Art. 725 of the Polish Civil Code, by a bank account agreement, the bank undertakes to keep the account holder for a fixed or indefinite period of time and, if the agreement so provides, to carry out cash settlements at his request. At this point, it should be clarified that the conclusion of a bank account agreement causes the holder's funds to become the property of the bank. Despite the lack of unambiguous wording in certain provisions of the act, there is a common and generally uncontroversial view in doctrine and jurisprudence that the bank obtains ownership of the deposited funds. As indicated, among others, by The Court of Appeal in Kraków in its judgment of February 5, 2014, file ref. (LEX no. 1 540 886), the bank account agreement is based on the structure of the irregular deposit (Art. 845 of the Polish Civil Code), which means that the bank acquires ownership of the funds contributed, and the bank account holder acquires a claim for the return of the amount resulting from provisions of the agreement linking the customer

19 See *Nieautoryzowane transakcje...*

with the bank. Thus, any operations performed on the bank account against the will of the account holder do not charge the account holder, but only the bank. Therefore, despite the fact that an unauthorized person extorts the property owned by the bank, there will be no damage to the account holder, as the bank will still be obliged to fully satisfy its claims from its own funds. The protection of claims is guaranteed to the holder by the provisions of civil and financial law and the agreement with the bank based on them (see the decision of the Supreme Court of April 28, 2016, file ref. (Legalis no. 1 442 847).

It should also be stated that the risk of making a withdrawal from a bank account to an unauthorized person and making a cash settlement on the basis of an instruction issued by an unauthorized person is borne by the bank, also when the bank account agreement is covered by internet banking (cf. judgment of the Court of Appeal in Warsaw of 19 July 2018 (LEX no. 1 822 123). The basis of the bank's liability in this respect are the legal norms contained in the Act of 19 August 2011 on payment services.

In view of the above, customers' demands for banks to fulfill their statutory obligations under Art. 46 sec. 1 of the Act of 19 August 2011 on Payment Services, i.e. the full refund of the unauthorized payment transaction amount, is fully justified.

Conclusions

Based on the research on payment frauds, it can be concluded that one of the biggest threats are social engineering and phishing attacks, often combined with the use of malicious software. User awareness campaigns are one of the most important remedial mechanisms against social engineering and phishing attacks that should be carried out by payment system institutions. Attacks using malicious software, and in particular ransomware, are becoming a more and more serious problem, which requires the use of new preventive actions and the use of measures to mitigate the effects of such attacks[20]. Preventing fraud in the payment system is not only a matter of indicating the payers' fault, but above all an institutional responsibility, where payment

20 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating counterfeiting and fraud related to non-cash means of payment, replacing Council Framework Decision 2001/413/JHA, Official Journal of the European Union 2019, L 123/18, Art. 17, prevention.

service providers should notice threats and possible emerging effects of their occurrence, which forces investing in appropriate security and monitoring technologies, as well as raising awareness of potential victims users.

The phenomenon of frauds related to non-cash means of payment is nowadays a significant threat to the security of the state and the security of the international environment, because frauds committed in the payment system are a source of income for actors of organized crime in supporting their activities in the field of terrorism, illegal drug and weapons trafficking, human trafficking and also APT type activities.

The weakest actors in the circumstances described above are individual citizens, individual clients of financial institutions, who become victims of computer crimes and often lose their life savings. Unfortunately, the conducted analyzes show that despite the existence of clear legal regulations protecting individual clients against the negative consequences of fraud carried out via computer networks, banks try to protect their own interests in the first place by transferring the negative effects of computer crimes to individual clients.

Bibliography

Duszczyk M., *Powraca najbardziej niszczycielski cyberwirus. Firmy mają powody do obaw*, „Rzeczpospolita" 2021, https://firma.rp.pl/biznes/art19126551-powraca-najbardziej-niszczycielski-cyberwirus-firmy-maja-powody-do-obaw-emotet-cyberwirus_IT [access: 10.09.2022].

2021 Payment Threats and Fraud Trends Report, Brussels 2021.

FBI: 6,9 miliarda dolarów – tyle w 2021 roku utracono z powodu przestępstw internetowych, CyberDefence24, Warszawa 2022, https://cyberdefence24.pl/cyberbezpieczenstwo/fbi-69-miliarda-dolarow-tyle-w-2021-roku-utracono-z-powodu-przestepstw-internetowych [access: 5.09.2022].

Final report. Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2), 2018, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20Article%2096%286%29%20PSD2%20%28EBA-GL-2018-05%29.pdf?retry=1 [access: 5.09.2022].

Janczak J., Pilarski G., Biernacik B., *Technologia informacyjna w zarządzaniu*, Warszawa 2009.

Komunikat ws. stosowania wyłączenia z art. 6 pkt 11 ustawy o usługach płatniczych (aktualizacja), Warszawa, 1 czerwca 2022, https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_ws_stosowania_wylaczenia_z_art_6_pkt_11_ustawy_o_uslugach_platniczych.pdf [access: 5.09.2022].

Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015.

Leżoń K., *Otwarta bankowość w świetle wymogów dyrektywy PSD2 – wyzwania i perspektywy rozwoju dla polskiego sektora FinTech*, Warszawa 2019.

Nieautoryzowane transakcje – zasady i główne problemy, Warszawa, 18 czerwca 2019, https://rf.gov.pl/wp-content/uploads/2020/05/Nieautoryzowane_trasnsakcje_analiza-RF_2019.pdf [access: 5.09.2022].

Ostrzeżenie przed dopuszczaniem pośredników do rachunku bankowego w płatnościach internetowych, Warszawa 2016, https://www.knf.gov.pl/knf/pl/komponenty/img/ostrzezenie_posrednicy_platnosci_60551.pdf [access: 10.09.2022].

Pilarski G., *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020.

Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, Warszawa 2015, https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf [access: 12.08.2022].

Rekomendacja dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa 2013.

Rekomendacje dotyczące bezpieczeństwa płatności internetowych, Frankfurt n. Menem 2013.

Cyberataki i odpowiedzialność banku za nieautoryzowane transakcje płatnicze w systemie bankowości internetowej – teoria i praktyka

Streszczenie

Artykuł dotyczy współcześnie spotykanych technik cyberataków skierowanych przeciwko bezpieczeństwu finansowemu banków i ich klientów oraz relacji banków z ich klientami na podstawie obowiązujących przepisów Unii Europejskiej (Dyrektywa Parlamentu Europejskiego i Rady UE 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego) i polskiej ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych. Autorzy analizują też stronę praktyczną relacji banków z ich klientami, którzy padli ofiarami oszustw komputerowych. Zwracają uwagę, że powszechnie stosowana przez banki praktyka polegająca na odmowie zwrotu środków skradzionych ich klientom w systemie bankowości elektronicznej jest niezgodna z obowiązującymi normami prawa polskiego i europejskiego.

Słowa kluczowe: cyberatak, bezpieczeństwo finansowe, system bankowości elektronicznej, oszustwo komputerowe, Unia Europejska

Krzysztof Marek Kiełpiński*

Informacja pozorna i fałszywa w jakościowej teorii informacji. Analiza z punktu widzenia cybernetyki

Streszczenie

Informacja jest podstawowym narzędziem komunikacji ***inter vivos***. Służy jako nośnik wielu danych. Funkcjonuje w wielu dziedzinach życia człowieka. Naukowcy z dziedziny cybernetyki zauważyli, że ludzkość ma trudności ze zdefiniowaniem pojęcia „informacja". Wielu badaczy podejmowało się tego zadania i próbowało stworzyć jej definicję. Na skutek przeprowadzonych badań udało się zdefiniować nie tylko pojęcie „informacja", ale również powstał dział nauki „jakościowa teoria informacji". Jej zadaniem było wskazanie natury informacji oraz przeprowadzenie analizy i syntezy tej ważnej rzeczywistości. Autor artykułu do prezentacji swoich rozważań wykorzystał różne metody badawcze, m.in.: historyczno-krytyczną, analityczną, filologiczną, matematyczną oraz dogmatyczno-prawną w celu pokazania obszarów, w których występuje specyficzny rodzaj informacji, tj. pozorna i fałszywa.

Przedmiot badania został poddany analizie, która doprowadziła autora do wskazania różnic między doktryną a nauką. Z punktu widzenia nauki naukowcy chcą, żeby ich poglądy pasowały do rzeczywistości. Doktrynerzy potrzebują rzeczywistości, żeby pasowała do ich poglądów. Zadaniem naukowca jest poszukiwanie prawdy, dlatego niepokoi go trudność jej znalezienia. Zwolennicy doktryny znają prawdę od początku i cieszą się jej kompletnością. Idąc dalej, naukowiec ma wiele wątpliwości, czy to, co mówi nauka jest prawdą, podczas gdy przedstawiciel doktryny nie ma wątpliwości, że to, co mówi doktryna jest prawdą. W końcu naukowiec uważa, że to, co mówi nauka jest nietrwałe, zatem doktryna odpowiada, że to, co mówi doktryna trwa wiecznie. Podstawowa kwestia została pokazana w różnych dziedzinach życia człowieka, w których pojawiają się różnego

* Ks. dr Krzysztof Marek Kiełpiński, Wydział Prawa Kanonicznego, Uniwersytet Kardynała Stefana Wyszyńskiego, e-mail: k.kielpinski28@gmail.com, ORCID: 0000-0001-8168-2514.

rodzaju informacje, wśród nich prawdziwe i fałszywe. Pseudoinformacje i dezinformacje występują bardzo często, dlatego w artykule przedstawiono ich podstawowe cechy i praktyczne ich zastosowanie.

Słowa kluczowe: informacja, informacja pozorna, informacja fałszywa, jakościowa teoria, symulacja, dysymulacja, konfuzyjny charakter informacji

Wstęp

Informacja jest podstawowym narzędziem, dzięki któremu jednostki się komunikują ze sobą. Za jej pomocą kształtują się relacje oraz więzi w społeczeństwie oraz pomiędzy ludźmi. Ma ona wpływ na naukę, poznanie świata, a także kształtowanie różnych istotnych doktryn. Staje się podstawowym kryterium poznania przez człowieka otaczającego go świata i dlatego odgrywa bardzo ważną rolę. Nie podlega dyskusji, że przekazywanie informacji zajmuje poczesne miejsce w życiu współczesnego człowieka. W tym obszarze następuje ciągła ewolucja. Wśród metod upowszechniania informacji od samego początku występowały: przemówienie do większej zbiorowości osób, rozmowa w cztery oczy, dyskusja, polemika, dialog, dyskurs, przypowieść, opowiadanie, porównanie, metafora, pytania retoryczne, emfaza, paralela, alegoria, hiperbola, poza lub gest. Wraz z rozwojem narzędzi komunikacyjnych powstały środki społecznego przekazu w postaci radia, telewizji, kina, prasy oraz plakatu. Ciągły rozwój doprowadził do stworzenia nowych środków komunikacji masowej, jak m.in.: internet, strony internetowe, DVD, Bluray, e-booki, e-prasa, telewizja cyfrowa, wiadomości – e-mail oraz SMS, social media, gry komputerowe, fora internetowe oraz fotografia cyfrowa[1].

Bardzo ważny aspekt dotyczy sposobu jej wyrażania i komunikowania. Właściwe „opakowanie" informacji będzie stanowiło punkt odniesienia dla wielu ważnych obszarów życia człowieka, społeczeństwa, wspólnot oraz organizacji międzynarodowych. Niewłaściwy sposób jej przesyłania może być powodem wybuchu wojny, wywołania kryzysu, a także śmierci wielu niewinnych ludzi. Artykuł jest poświęcony informacji pozornej i fałszywej, ponieważ współcześnie stanowią one główne narzędzie do wywoływania chaosu w przestrzeni społecznej. Ponadto różne informacje, niekiedy nieprawdziwe,

1 J. Krajczyński, *Wystąpienia wiernych w mass mediach w sprawach wiary i obyczajów* [w:] *Fides, quae de verbo nascitur et nutritur. Nauczycielskie zadanie Kościoła wobec 1050 rocznicy chrztu Polski*, red. J. Krajczyński, A. Domaszk, Płock 2016, s. 110–111.

są umieszczane w przestrzeni wirtualnej w jednym celu – kształtowania światopoglądu, a także opinie ludzi. Celem studium będzie ukazanie różnych rodzajów informacji w jakościowej teorii informacji, a także negatywnych skutków jej rozpowszechniania i powielania w świecie rzeczywistym i w mass mediach.

Informacja – próba określenia definicji

Poszukując definicji informacji, należy zatrzymać się nad stwierdzeniem Hansa Joachima Flechtnera. Ten wybitny niemiecki naukowiec zauważył, że „[...] pojęcie informacji jest nie tylko centralnym pojęciem teorii informacji, lecz także jednym z podstawowych pojęć cybernetyki. Zarazem jest ono z pewnością najtrudniejszym pojęciem dla tego, kto chce wgłębić się w cybernetykę. Przegląd literatury pokazuje, że nie tylko bardzo różnie jest definiowana, lecz jest pojęciem, które w ścisłej definicji teorii informacji wydaje się mieć zupełnie inne znaczenie niż to, które zwykliśmy znać na co dzień i się nim posługiwać”[2]. Myśl Flechtnera w polskiej myśli nad jakościową teorią informacji zgłębił i rozwinął Marian Mazur. Jego zdaniem najpierw należy rozpocząć działania, które pozwolą odnaleźć naturę lub istotę informacji. Badania należy rozpocząć od zbadania ilości informacji. Uzyskana w ten sposób wiedza pozwoli dotrzeć do właściwych elementów tworzących definicję pojęcia „informacja”. Do określenia ilości informacji ten wybitny polski naukowiec wykorzystuje wzór matematyczny Claude'a Shannona[3]. Stanowi podstawę ilościowej teorii informacji, gdzie entropię zbiorową n prawdopodobieństw p_1, p_2, p_3 (możliwa nieskończona liczba przypadków) i określająca ją liczbowo ilość informacji $H = -\sum_{i=1}^{n} p\ i \log p\ i$. Gdy H będzie wynosiła zero – według Mazura – można mówić, że przekazywana ilość informacji jest pewna i prawdziwa[4]. Matematyczne spojrzenie na naturę informacji nie przyniosło skutecznego rozwiązania, ponieważ wielu humanistów nie potrafiło zrozumieć matematycznych zależności i zasad. Mazur stwierdza, że praca Shannona dotyczy raczej przekazywania przenoszących informację sygnałów, a nie informację *in genere*[5].

2 H.J. Flechtner, *Grundbegriffe der Kybernetik*, Stuttgart 1966, s. 20–21.
3 C. Shannon, *A mathematical theory of communication*, „The Bell System Journal” 1948, nr 27, s. 397–423.
4 M. Mazur, *Jakościowa teoria informacji*, Warszawa 1970, s. 15.
5 Ibidem, s. 18.

Poza matematycznymi rozwiązaniami również humaniści poszukiwali definicji pojęcia „informacja". Literatura światowa prezentowała różne teorie. W związku z tym należy wyróżnić trzy ich grupy. Pierwsza utożsamia pojęcie „ilość informacji" z terminem „informacja". Tego typu praktyka została skrytykowana przez Mariana Mazura oraz Colina Cherry'ego. Obaj twierdzą, że utożsamienie tych dwóch obszarów ze sobą wyklucza tych badaczy, którzy chcą przeprowadzić badania tylko związane z ilością informacji. Cherry stwierdził, że „[...] w pewnym sensie należy żałować, że matematyczne pojęcie zostało ogólnie nazwane informacją"[6]. Drugą grupę tworzą artykuły, w których pojawia się termin „informacja". Niestety, nie ma on żadnych wyjaśnień, jakby nie budził żadnych wątpliwości. Trzecia grupa publikacji próbuje wyjaśnić pojęcie „informacja". Niektórzy autorzy ograniczają swoje wyjaśnienia do paru zdań, inni przeprowadzają rozległe dyskusje. Istnieje mała grupa, która próbuje pokazać trudności w stworzeniu definicji oraz porównuje poglądy różnych autorów, żeby czytelnik potrafił wyrobić sobie własne zdanie na ten temat. Norbert Weiner wykorzystuje metodę negatywną, żeby pokazać, czym nie jest informacja. Stwierdza, że „[...] mechaniczny mózg nie wydziela myśli, jak wątroba wydziela żółć, zdaniem dawniejszych materialistów, ani też nie wydaje jej w postaci energii, jak to robi mięsień w swoim działaniu. Informacja jest informacją, a nie energią lub materią"[7]. Następnie podaje definicję informacji jako treści zaczerpniętej ze świata zewnętrznego w miarę jak się do niego dostosowujemy i jak przystosowujemy do niego swoje zmysły[8].

Zdaniem Mazura definicja jest niekompletna, ponieważ definicję określa słowo „treść", które ma charakter nieokreślony i jest pozbawione ogólności[9]. Określenia definicji „informacja" podjął się Louis Couffingal. Stwierdził, że informacją nazywa się działanie fizyczne, któremu towarzyszy działanie psychiczne. W definicji można wyróżnić dwa elementy, tj. semantykę i nośnik. Semantyka stanowi efekt psychiczny informacji, a nośnik to zjawisko psychiczne skojarzone z semantyką w celu tworzenia informacji[10]. Skrupulatna analiza definicji Couffingala przeprowadzona przez Mazura wykazała trzy poważne mankamenty. Po pierwsze, definicja jest zbyt szeroka. Autor rekapituluje, że

6 C. Cherry, *On human communication. A revive, a survey and criticism*, Massachusetts 1966, s. 34–35.
7 N. Weiner, *Cybernetics or control communication in the Animal and the Machine*, New York 1948, s. 45–67.
8 Ibidem, s. 70.
9 M. Mazur, *Jakościowa teoria...*, s. 20.
10 L. Couffingal, *La Cybernetique*, Paris 1963, s. 31–52.

w cybernetyce działanie psychiczne jest tak samo fizyczne jak każde inne. Druga uwaga dotyczy relacji semantyki do informacji. Informacja jest zdefiniowana przez semantykę, a semantyka przez informację. Odwołanie się do działania psychicznego pozbawiało definicję ogólności. Trzecia dotyczy niekonsekwencji stosowania terminu „informacja". Mazur stwierdził, że informacje zawarte w tekście początkowym pozostały takie same, chociaż zmieniła się ich forma. Można przekonać się, że informacja nie jest traktowana jako zespół nośnika i semantyki, lecz jako odrębna od nośnika[11].

Kolejną próbę podania definicji informacji podjął się Hans Joachim Flechtner. Twierdzi on, że informacja to sygnał (*signal*), który może, ale nie musi zawierać lub przenosić wiadomości (*nachricht*). Tego typu określenie może być różnie traktowane przez odbiorcę. Po pierwsze, odbiera tylko jako sygnał, lecz nie jako wiadomość. Po druga, odbiera wiadomość, ale jej nie rozumie. Po trzecie, umożliwia zrozumienie wiadomości, ale ona nie interesuje odbiorcę lub jest mu obojętna. Ostatnia to taka, że wiadomość odebrana ma wartość i znaczenie dla odbiorcy. Mazur krytykuje definicję zaproponowaną przez Flechtnera, ponieważ nie wiadomo co jest naturą wiadomości. Ponadto wyjaśnienie definicji „informacja" przez termin „informowanie" to tautologia[12].

Wyjaśnienia pojęcia „informacja" podjął się również Mazur. Wykorzystał do jej stworzenia zasady i reguły, którymi posługiwała się cybernetyka. Jej cechą charakterystyczną jest transdyscyplinarne podejście do systemów sterowania oraz przekazywania informacji w człowieku i maszynie[13]. Według niego informacja jest to transformacja jednego komunikatu asocjacji informacyjnej w drugi komunikat tej asocjacji. Komunikat jest to stan fizyczny, który różni się w określony sposób od innego stanu fizycznego w torze sterowniczym. Asocjacja komunikacyjna to transformacja, której należy poddać jeden komunikat, żeby otrzymać drugi. Transformacja to proces, któremu należy poddać jeden z komunikatów asocjacji, żeby otrzymać drugi komunikat tej asocjacji. Powyższe przykłady pokazały, że bardzo trudno było stworzyć definicję informacji. Mając na uwadze elementy definicji opracowanej przez Mazura, warto podkreślić, że jest ona ogólna. Będzie stanowić punkt wyjścia do dalszej analizy poświęconej informacji operacyjnej, która odgrywa szczególną rolę. Zostaną pokazane ponadto jej różne rodzaje[14].

11 M. Mazur, *Jakościowa teoria*..., s. 20–21.
12 Ibidem, s. 21–22.
13 M. Mazur, *Cybernetyka i charakter*, Warszawa 1976, s. 5–22.
14 Idem, *Jakościowa teoria*..., s. 70–80.

Informacja operacyjna i zasadnicza

Informacja operacyjna to działanie stanowiące transformację operacyjną. Zawarty w informacji kod występuje w różnorakich pomiarach. Mazur wskazuje, że klasycznym rodzajem tego typu informacji są działania matematyczne. Rodzajem operacji jest mnożenie, a jej parametrem liczba wskazująca wielkość mierzoną. Na tej podstawie można stwierdzić, że informacja operacyjna polega na przekazaniu wielkości mierzonej, która jest większa od jednostki miary tej wielkości. Może ona przybrać również inną postać. Działanie tego typu nosi nazwę „informacja operacyjna odwrotna" i polega na transformacji operacyjnej odwrotnej do danej informacji operacyjnej. Wykorzystywana jest w kartografii oraz naukach geograficznych, które mają na celu ustalić odległości pomiędzy państwami lub miastami. Zobrazowuje to stwierdzenie, że Sztokholm leży 1300 km na północ od Budapesztu. Informacją odwrotną będzie stwierdzenie, że Budapeszt leży 1300 km na południe od Sztokholmu[15]. Informacjami operacyjnymi i operacyjnymi odwrotnymi są zmiany wyrazów w deklinacjach oraz koniugacjach. Informacje operacyjna i operacyjna odwrotna stanowią podstawę informacji zasadniczej oraz zasadniczej odwrotnej. Informację zasadniczą określa się jako operacyjną jednakową dla wszystkich kolejnych asocjacji łańcucha informacyjnego. Informacja zasadnicza odwrotna stanowi transformację do danej informacji zasadniczej. Mazur podkreśla, że informacja zasadnicza wymaga dwóch elementów, tj. rodzaju operacji oraz parametru operacji[16]. Poszukiwanie jej polega na tym, że najpierw zakłada się pewien rodzaj operacji, po czym określa się parametr na podstawie kolejnych komunikatów. Po analizie dalszych wypowiedzi polskiego cybernetyka dochodzi się do wniosku, że szukanie informacji zasadniczej może okazać się mozolne. Szukanie jej w zjawiskach fizycznych jest utrudnione, dlatego że dane fizyczne pochodzą z pomiarów, które są obarczone błędami. Przykładem informacji zasadniczej w odniesieniu do struktury komunikatów liczbowych jest informacja operacyjna polegająca na dopisywaniu zera podczas mnożenia przez dziesięć lub przesuwaniu przecinka w ułamkach dziesiętnych. Informacje w strukturach wyrazów mają znikome zastosowanie. Innym przykładem może być dodawanie przedrostka. Informacja operacyjna słowa „wnuk" poprzez dodanie przedrostka „pra-" tworzy informację zasadniczą jako prawnuk

15 Ibidem, s. 75.
16 Ibidem, s. 79.

lub praprawnuk. Podobny proces dokonuje się ze słowem „informacja". Przez dodanie przedrostka „meta-" tworzy się informację zasadniczą w postaci słów „metainformacja" oraz „metametainformacja"[17].

Pseudoinformowanie – informacja pozorna

Bardzo ważnym elementem tworzenia informacji pozornej jest pseudoinfomowanie, które należy na wstępie szczegółowo wyjaśnić. Pseudoinformowanie jest to proces informowania, w którym niektóre komunikaty są wspólne dla kilku łańcuchów kodowych. Pseudoinformacja jest to proces, w którym informacja jest umieszczona w obrazach na skutek pseudoinformowania. Działania te mogą przybrać różne formy: symulacji, dysymulacji oraz konfuzji. Symulacyjny charakter pseudoinformowania polega na tym, że niektóre łańcuchy kodowe mają wspólny oryginał, lecz różne obrazy. Jest to efekt pseudoinformowania symulacyjnego.

Najprostsza forma pseudoinformowania symulacyjnego powstaje wówczas, gdy ta sama przyczyna wywołuje różne skutki. Posługując się językiem analogii, ma to miejsce wtedy, kiedy jedna choroba wywołuje różne objawy[18]. Symulacyjny charakter pseudoinformowania opiera się na analizie. Przeprowadzona analiza wyróżnia w niej przypadki, które są zbiorem obrazów zawierających informacje pozorne. Tego typu przekaz nie wnosi nic nowego do obiektu analizowanego. W naukach fizycznych przykładem takiej analizy jest rozszczepienie światła białego za pomocą pryzmatu. Otrzymane barwy są dostrzegalne, podczas gdy w świetle białym są niedostrzegalne przez ludzkie oko. Ten sam mechanizm funkcjonuje, gdy następuje użycie wyłącznika elektrycznego, co wywołuje zaświecenie lampy, lub naciśniecie klawisza, który uruchomia dźwięk dzwonka do domu. Te dwa sygnały stanowią obrazy informacji pozornej, ponieważ informacją zasadniczą i operacyjną jest to, że w obu przypadkach obwody elektryczne są sprawne[19].

17 Ibidem.

18 *Stwardnienie rozsiane – jedna choroba, różne objawy*, https://stylzycia.polki.pl/choroby,stwardnienie-rozsiane-jedna-choroba-rozne-objawy,10409555,artykul.html [dostęp 13.06.2022]; *Cukrzyca – jedna choroba, różne oblicza*, https://przychodnia-skala.pl/dla-pacjenta/profilaktyka/cukrzyca-jedna-choroba-rozne-oblicza [dostęp 13.06.2022].

19 M. Mazur, *Cybernetyka i charakter*..., s. 84–85; M. Geppert, *Uwagi o koncepcji dwóch systemów sygnałowych*, „Studia Filozoficzne" 1961, nr 4, s. 65–102.

W humanistyce działania pseudoinformacyjne w wymiarze symulacyjnym występują bardzo często. W językoznawstwie analiza głosek stanowi tego najlepszy przykład. Głoskę „h" można zapisać na wiele sposobów w postaci litery „h" napisanej prosto, kursywą, większymi lub małymi czcionkami o różnych proporcjach. To wszystko jest informacją pozorną symulowaną, która nie zmienia tego, że chodzi o głoskę „h", a nie o jakieś inne[20]. W powieściach lub opowiadaniach tego typu informacja jest używana za pomocą wyrazów równoznacznych. Nie wzbogacają one treści, ale są używane po to, żeby urozmaicić stylistykę[21].

Informację pozorną symulacyjną wykorzystują mówcy: politycy, duchowni, konferansjerzy, mówią o tym samym za pomocą coraz to innych sformułowań, żeby sprawić wrażenie, że ma się do czynienia z bogactwem słownictwa i unikatowością przekazu. Najlepiej podsumowuje to łacińskie sformułowanie: „Ut aliquid scripsisse (dicitisse) videatur"[22]. Ponadto ten rodzaj informacji występuje w publikacjach naukowych. Autorzy posługują się wyrazami równoznacznymi w swoich dziełach. W ten sposób doprowadzają do chaosu i dezorientacji swoich czytelników. Jeżeli czytelnik zna jedną nazwę danego pojęcia, a w literaturze spotka się z inną użytą w podobnym kontekście, to naturalną rzeczą jest występowanie wątpliwości. Czytelnik będzie zadawał sobie różne pytania, czy to przejaw skłonności autora do urozmaiceń stylistycznych czy raczej chodzi o dwa różne pojęcia[23].

Kolejny wymiar pseudoinformowania to dysymulacja. Dysymulacyjny charakter informacji wskazuje, że niektóre łańcuchy kodowe mają wspólny obraz, lecz różne oryginały. Skutkiem jest informacja dysymulacyjna, którą można określić jako informację pozorną ogólną. Można się z nią spotkać wówczas, gdy różne przyczyny wywołują taki sam skutek. W medycynie wskazuje się różne choroby, które mają wspólne objawy[24]. Zadaniem procesu dysymulacji jest dokonanie syntezy, a wynikające z niej uogólnienia stanowią pseudoinformację dysymulacyjną, która zaciera granice pomiędzy szczegółem a ogółem. Występuje ona w naukach matematycznych, gdzie na przykładzie

20 M. Mazur, *Cybernetyka a humanitaryzm*, „Argumenty za i przeciw" 1963, nr 4, s. 32–42.
21 Ibidem, s. 36.
22 L. Czapliński, *Księga przysłów, sentencji i wyrazów łacińskich*, reprint, Warszawa 1987, s. 492; S. Kalinowski, *Scire Latine. Język łaciński. Podręcznik dla alumnów i studentów teologii*, Warszawa 2014, s. 220.
23 P. Siuda, P. Wasylczyk, *Publikacje naukowe*, Warszawa 2018, s. 75–81; B. Śliwierski, *Habilitacja: diagnoza – procedury – etyka – postulaty*, Kraków 2017, s. 196–204.
24 A. Comfort, *Biological Aspects of Senescence*, „Biological Reviews" 1954, nr 29, s. 284–329.

pojęć szczególnych, m.in. trójkąty równoboczny, równoramienny, prostokątny, ostrokątny lub rozwartokątny, tworzy się pojęcie ogólne „trójkąt”[25]. Wielokrotnie stosuje się w socjologii lub statystyce. Dane statystyczne, jako sumarycznie przedstawiające grupy poszczególnych obiektów, zawierają informację pozorną ogólnikową[26]. Tocząca się wojna pomiędzy Federacją Rosyjską a Ukrainą jest kolejnym przykładem wykorzystania pseudoinformowania dysymulacyjnego. W trakcie toczącego się konfliktu sporządza się meldunki wojskowe na temat ponoszonych strat podczas wojny. Na poziomie plutonu wymienia się personalia poległych, a na poziomie pułku już tylko podaje się liczbę poległych szeregowców, podoficerów i oficerów. Na poziomie armii podaje się liczbę poległych i to w tysiącach żołnierzy[27]. Inny przykład z tego obszaru to komunikaty typu: „dwa plutony dostały się do niewoli”, „żołnierze się poddali”, „armia dopuściła się masakry ludności”. Z tego typu informacji nie wiadomo, których wojsk one dotyczą, agresora czy broniących się[28]. W związku z tym można zaobserwować, że pseudoinformacja dysymulacyjna powoduje ubytek informacji. Pożytecznym zadaniem, które ma do spełnienia, jest to, że umożliwia uniknięcie trudności mogących wynikać z występowania dużej ilości danych. Użycie jej zależy od tego, które dane są potrzebne do jasnego i ogólnego przekazu. Należy podkreślić, że dysymulacyjny charakter informacji jest szkodliwy, ponieważ uniemożliwia porównanie ze sobą szczegółów[29].

W szeroko pojętej humanistyce pseudoinformacja dysymulacyjna polega na używaniu wyrazów wieloznacznych. Mogą one prowadzić do nieporozumień, szczególnie jest to odczuwalne w publikacjach naukowych. Zadaniem

25 L. Brillouin, *Science and Information Theory*, New York 1956, s. 56–60.

26 https://stat.gov.pl/ [dostęp: 13.06.2022].

27 https://wiadomosci.wp.pl/wojna-w-ukrainie-kazdy-metr-ziemi-jest-zlany-krwia-dramatyczny-apel-do-usa-relacja-na-zywo-6779143955548864a [dostęp: 13.06.2022].

28 Sun Tzu, Sun Pin, *Sztuka wojny*, Gliwice 2021, s. 273–279.

29 Materiały dotyczące pedofilii w Kościele katolickim na świecie i Polsce. Reportaże, które przeważnie mają wymiar ogólnikowy, bez wskazania szczegółowych dowodów winy zob. https://tvn24.pl/go/szukaj/36?q=czarno+na+bia%C5%82ym [dostęp: 20.05.2022]. Więcej na ten temat w reportażach Marcina Gutowskiego dla magazynu „Czarno na Białym” TVN24 opublikowanych w latach 2019–2021, m.in.: „Cena cierpienia”; „Demon w Watykanie”; „Dzieci nie tego Boga”; „Purpurowa sieć”; „Królestwo. Postscriptum”; „Sojusz tronu z ołtarzem”; „Królestwo w Orchard Lake”; „Sygnał ostrzegawczy dla Kościoła”; „Twarze arcybiskupa Gądeckiego”; „Don Stanislao. Druga twarz kardynała Dziwisza”; „Mecenas Artur Nowak. Kościół chce być wyjęty spod prawa”; „Kościół nie zrobi nic, to jest problem społeczny, który powinno rozwiązać państwo”; „Potęga księdza Dymera”; „Najdłuższy proces Kościoła”; „Zarzuty pod adresem abp. Leszka Sławoja Głodzia”; „Historia Maciela Degollado”; „O kulisach siostry Joanny”.

komisji terminologicznych w rozmaitych dziedzinach wiedzy jest wprowadzanie nowych pojęć, co przyczynia się do usuwania terminów wieloznacznych. Można zauważyć, że osoby niekompetentne w konkretnej dziedzinie posługują się ogólnymi sformułowaniami. Przykładem są debaty publiczne, debaty przed wyborami prezydenckimi, debaty społeczne, demonstracje oraz strajki[30]. W przestrzeni uniwersyteckiej można doświadczyć tego typu zdarzenia podczas sesji egzaminacyjnych. Student, który nie przygotował się do egzaminu, poproszony o szczegółowe wyjaśnienie problemu będzie posługiwał się ogólnikami, ponieważ nie jest ich pewny lub nie chce zdradzić ich nieznajomości. Informacja pozorna ogólnikowa ma zastosowanie podczas tworzenia notatek, opinii lub sporządzania protokołu. Wykorzystują ją jako narzędzie służby specjalne, członkowie rad nadzorczych, komisji rewizyjnych, rad pedagogicznych wtedy, kiedy należy zaprotokółować przebieg zdarzenia lub spotkania[31].

Blaski i cienie psuedoinformowania dysymulacyjnego stanowią punkt wyjścia do pokazania trzeciego rodzaju informacji pozornej – pseudoinformowania konfuzyjnego. Można ją podzielić na informację pozorną konfuzyjną pojedynczą oraz podwójną. Psuedoinformowanie konfuzyjne sprawia, że niektóre łańcuchy kodowe mają wspólne cechy oryginałów i obrazów. Mówiąc potocznie, jest to kombinacja pseudoinformacji symulacyjnej i dysymulacyjnej. Cechą charakterystyczną w tym przypadku jest to, że jeden z możliwych skutków z jakiejś przyczyny może powstać również z innej przyczyny. Występuje w medycynie, gdy jeden z objawów pewnej choroby może być zarazem objawem innej choroby. Można się z nim spotkać w związku z tendencją do określania funkcji zawodowych, dawniej niedostępnych dla kobiet – jedna nazwa bez względu na płeć, m.in. profesor, doktor, minister, ambasador. Tendencja ta rozszerza się również na funkcje zawodowe, dla których istnieją osobne nazwy dla mężczyzn i kobiet, m.in. nauczyciel–nauczycielka, aktor–aktorka; tancerz–tancerka; kierownik–kierowniczka. W związku z tym używanie ich staje się informowaniem konfuzyjnym pojedynczym, ponieważ nauczająca kobieta bywa wielokrotnie nazywana nauczycielem i nauczycielką, a zarazem wyraz „nauczyciel" może oznaczać nauczającego zarówno mężczyznę, jak i kobietę. Powyższy przykład stanowi kombinację pseudoinformacji symulacyjnej i dysymulacyjnej[32].

30 https://www.youtube.com/watch?v=_1ZlSDDuXwE, https://www.youtube.com/watch?v=zoOzG4gjGck; https://www.youtube.com/watch?v=B-JkbvOgdLE [dostęp: 13.06.2022].
31 M. Netzley, C. Snow, *Pisanie raportów*, Warszawa 2009, s. 1–93.
32 M. Mazur, *Jakościowa teoria...*, s. 127–128.

Pseudoinformowanie konfuzyjne podwójne występuje wówczas, gdy każdy z rozpatrywanych skutków może być wywołany przez każdą z przyczyn. Tego typu zjawiska można spotkać w medycynie lub w dawnych sztukach teatralnych, gdzie aktor grał dwie role, które miały wywołać efekt humorystyczny, refleksyjny lub twórczy, a także w publicystyce podczas przekazywania faktów[33]. Powyższe rozważania mają wskazać, że pseudoinformowanie dysymulacyjne jest skutecznym środkiem ukrywania prawdy bez narażenia się na zarzut kłamstwa, zwłaszcza wtedy, kiedy osoba jest zmuszana do odpowiadania na pytania. Ogólnikowe odpowiedzi stanowią obszerny katalog możliwości, co przepytującemu utrudnia lub uniemożliwia znalezienie właściwej informacji[34].

Dezinformowanie – informacja fałszywa

Marian Mazur zauważa, że proces dezinformacji ma na celu oddzielić wszystkie łańcuchy kodowe. Niestety, należy stwierdzić, że w tym procesie niektóre dane nie są pełne. Idąc drogą wskazaną przez polskiego uczonego, należy podkreślić, że pod pojęciem „dezinformowanie" kryje się czynność, która tworzy łańcuchy zawierające kody (dane) jako niepełne struktury[35]. Dezinformacja tworzy rodzaj informacji, w której brakuje obrazów w zbiorze go tworzącym. Tego rodzaju informacja może przybrać postać: symulacyjną, dysymulacyjną i konfuzyjną.

Symulacyjny wymiar dezinformacji występuje m.in. poprzez stworzenie fałszywych dokumentów, wykorzystanie cudzych podpisów, tworzenie tzw. legendy dla oficera wywiadu, sporządzanie fałszywych pokwitowań, tworzenie nieprawdziwych meldunków, alarmowanie o zagrożeniu, mimo że w rzeczywistości ono nie występuje[36]. W dobie konfliktu Federacji Rosyjskiej z Ukrainą przykładem symulacyjnego wymiaru dezinformacji jest podawanie w mass mediach informacji o możliwości wybuchu wojny na terenie Rzeczypospolitej

33 Ibidem.
34 K. Jaspers, *Problem winy*, Warszawa 2018, s. 65–84.
35 M. Mazur, *Jakościowa teoria...*, s. 140–141.
36 B. Piasecki, *Kontrwywiad, atak i obrona*, Łomianki 2021, s. 244; A. Kowalski, *Kontra. Sztuka walki z wywiadem przeciwnika*, Łomianki 2021, s. 57–97; H. Munkler, *Wojny naszych czasów*, Kraków 2004, s. 97–110.

Polskiej, pokazywanie ćwiczeń wojskowych wojsk rosyjskich i białoruskich przeprowadzonych na Białorusi w kontekście potencjalnej wojny z Polską[37].

W dziedzinie sądownictwa przykładem może być oświadczenie oskarżonego, który w celu uchronienia od kary bliskiej mu osoby, będącej rzeczywistym sprawcą przestępstwa, przyznaje się do przestępstwa przez siebie niepopełnionego albo zeznania świadka, który kłamie i zmyśla fakty niezaszłe lub opisuje to, co było zwykłym przewidzeniem. Podczas zakupów klient może zderzyć się z tego rodzaju dezinformacją, zwłaszcza wtedy, kiedy w cenniku został wymieniony towar, chociaż w rzeczywistości wcale go nie ma w sprzedaży. Podobne informacje można spotkać w rozkładach jazdy kolejowym, lotniczym lub autobusowym, w których widnieje godzina odjazdu lub przyjazdu środka transportu, a w rzeczywistości wcale on nie kursuje[38].

Główny obszar, w którym występuje ten rodzaj dezinformacji, to propaganda. Można mnożyć przykłady w tej dziedzinie. Przejawem tego są komunikaty, w których występują wzmianki o zwycięskich walkach niemających miejsca. Innym przykładem dezinformacji są sytuacje, gdy rządy lub przedstawiciele krajów zarzucają przeciwnikom wrogie wystąpienia, które nie miały miejsca, gdy partie polityczne atakują swoich przeciwników za słowa niewypowiedziane. Prasa, radio, telewizja, portale informacyjne w celu wzbudzenia zainteresowania odbiorców podają zmyślone sensacyjne wiadomości. Kolejny przykład dezinformacji to koncerny, które za pomocą reklamy wychwalają swoje wyroby i przypisują im różne właściwości, których one w ogóle nie mają. Z tym rodzajem dezinformacji można się zetknąć podczas czytania powieści, oglądania filmów lub spektakli teatralnych[39].

Jako kontratyp oraz rodzaj ekskulpacji umieszcza się stwierdzenie, że wszystkie postacie zostały zmyślone, a ewentualne podobieństwo do rzeczywistych osób jest całkowite przypadkowe. W ten sposób unika się kosztownych procesów sądowych ze strony tych, którzy mogliby czuć się dotknięci podobieństwem do postaci przedstawianych w powieści, sztuce teatralnej lub filmie[40].

Drugi rodzaj dezinformacji ma charakter dysymulacyjny. Proces zakłada, że niektóre łańcuchy kodowe w ogóle nie zawierają obrazów. W ten sposób

37 K. Kiełpiński, *Decepcja jako fundamentalne narzędzie pracy służb specjalnych w ramach wojny hybrydowej*, https://disinfodigest.pl/decepcja-jako-narzedzie-pracy-sluzb-specjalnych-w-ramach-wojny-hybrydowej/ [dostęp: 13.06.2022].
38 M. Mazur, *Jakościowa teoria...*, s. 142.
39 Ibidem, s. 143.
40 Ibidem.

przerywa się przesyłanie danych i tworzenie informacji. Przykładem dezinformacji dysymulacyjnej jest przypadek, który może pojawić jako niezamierzone działanie. W dziedzinie sprawiedliwości i bezpieczeństwa jest nim przestępca, który niszczy kompromitujące dowody albo zaciera ślady swojego pobytu w miejscu przestępstwa, świadek, który celowo zataja fakty albo o nich zapomina. Z innymi przykładami, które codziennie występują w różnych obszarach aktywności ludzkiej, spotykamy się w sklepach – w cenniku nie został wymieniony towar, który w rzeczywistości jest dostępny w sprzedaży. Podobna sytuacja może mieć miejsce z kursami jazdy autobusów, pociągów i samolotów – w rozkładach jazdy brakuje informacji o dacie i godzinie odjazdu, a w rzeczywistości środek transportu wykonuje zaplanowany kurs[41].

Podczas przeglądania portali internetowych, słuchania radia lub oglądania telewizji można natrafić na ten rodzaj dezinformacji. Strony obecnego konfliktu na Ukrainie w komunikatach wojennych zaniżają własne porażki i poniesione straty w ludziach i sprzęcie. W historii XX wieku z tego rodzaju informacją fałszywą powinno kojarzyć się podpisanie traktatu o nieagresji pomiędzy III Rzeszą a ZSRR 23 sierpnia 1939 roku. Działanie polegało na zatajeniu podziału ziem II Rzeczypospolitej, stanowiącego załącznik do podpisanego paktu Ribbentrop–Mołotow[42].

Tego typu działanie (dezinformację dysymulacyjną) można powstrzymać, czego najlepszym przykładem jest formuła sądowa stosowana do stron sporu oraz świadków. Brzmi ona: „Strona/świadek będzie mówił prawdę, całą prawdę i tylko prawdę". Analiza tego sformułowania wskazuje, że strona lub świadek wobec sądu zobowiązują się do informowania zasadniczego oraz wyrzekają się dezinformacji w wymiarze symulacyjnym (tylko prawdę) i dysymulacyjnym (całą prawdę).

Dezinformację dysymulacyjną wielokrotnie wykorzystują oficerowie różnych wywiadów. Złapani przez służby obcego państwa i przesłuchiwani pod wpływem nacisku korzystają z tego typu działania. Dysymulacja jest bezpieczniejsza, ponieważ zmyślanie jest na ogół znacznie łatwiejsze do wykrycia niż zatajenie, dlatego że fakty zatajone są wypytującemu nieznane, nie wie on, co ma sprawdzać. Gdyby je znał, to nie pytałby o nie, z wyjątkiem przypadku, w którym chodzi jedynie o sprawdzenie prawdomówności wypytywanego, czyli o wypowiedzi mającej służyć jako komunikaty rozpoznawcze. Ostatnim

41 Ibidem, s. 144.
42 Ibidem, s. 145.

obszarem jej wykorzystania jest propaganda. Wykorzystuje się do tego obszar cybernetyczny i przestrzeń online. Rozwój teleinformatyczny umożliwia rozgłaszanie wiadomości bardzo szybko i bardzo wielu ludziom jednocześnie, z wykorzystaniem dysymulacyjnego wymiaru dezinformacji. W ten sposób umożliwia się przemilczanie kompromitujących faktów, opinii i okoliczności o przeciwnikach politycznych, wrogach społecznych, grupach etnicznych, jednostkach czy aferach[43].

Ostatnim rodzajem dezinformacji jest dezinformacja konfuzyjna. Polega ona na tym, że informacja w łańcuchach danych (kodach) nie zawiera oryginałów oraz obrazów, jest kombinacją dezinformacji symulowanej i dysymulowanej. Występują dwie jej odmiany, tj. pojedyncza i podwójna. Dezinformacja konfuzyjna pojedyncza najczęściej związana jest z ludzką słabością. Człowiek wielokrotnie popełnia pomyłki, jest niedokładny i nonszalancki. Występuje najczęściej na skutek ludzkiego błędu. Można się z nią spotkać, gdy rozkład jazdy autobusów, samolotów, pociągów i innych środków transportu zawiera – na skutek ludzkiego błędu – inną godzinę odjazdu lub przyjazdu, w sklepie, gdy w cenniku została umieszczona niewłaściwa cena jakiegoś towaru, a także wtedy, kiedy podamy komuś zły numer telefonu lub zły adres zamieszkania. Inną odmianą są przeinaczenia. Mogą one występować, gdy nastąpiło m.in. przerobienie cyfr na czeku lub pokwitowaniu, gdy ktoś występuje pod fałszywym nazwiskiem, gdy w zestawieniu lub bilansie widnieją różne kwoty. W dziedzinie sądownictwa może się ono pojawić, gdy świadek zeznaje, że pobitego uderzono ręką, a nie innym narzędziem. Stanowi to kombinację dezinformacji symulacyjnej z dysymulacyjną. Jeżeli świadek zataił uderzenie innym narzędziem, to będzie to rodzaj dezinformacji dysymulacyjnej, jeżeli zaś świadek wymyślił, że nastąpiło uderzenie ręką, to należy mówić o dezinformacji symulacyjnej[44].

W trakcie trwającego konfliktu na Ukrainie odpowiedzialni za informacje podawali dane, w których wykazywali małe straty własne na tle dużych strat nieprzyjaciela[45]. Niekiedy z tego typu działaniami można spotkać się w podręcznikach historii, gdzie daty i wydarzenia zostały przeinaczane, m.in. wydarzenia z najnowszej historii Polski: sprawa katyńska z 1940 roku, żołnierze wyklęci w latach 1945–1956, początki ruchu NSZZ „Solidarność"

43 Ibidem.
44 Ibidem, s. 146–147.
45 Ibidem.

w 1980 roku[46]. Z nią można spotkać się w pracy oficerów wywiadu, gdy muszą przejąć wrażliwe dokumenty i w ich miejsce umieścić inny dokument. Najczęściej występuje w ludzkiej codzienności w postaci plotek o innych osobach. To cenne źródło wiedzy o osobie i jej zachowaniu. Najczęściej odbiega ona od rzeczywistego stanu rzeczy, mimo że niektórzy podkreślają, że w każdej plotce jest ziarenko prawdy.

Ostatnią kwestią, do której należy się odnieść, jest rodzaj dezinformacji konfuzyjnej podwójnej. Jest to połączenie dezinformacji symulacyjnej i dysymulacyjnej. Przeważnie występuje w sądownictwie oraz podczas przekazywania informacji przez media z konfliktów wojennych. W trakcie rozprawy świadek zeznaje kłamliwie lub wskutek pomieszania osób, że Tomek uderzył Krzysztofa, podczas gdy to Krzysztof uderzył Tomka. Analizując to, można wyróżnić dwie dezinformacje symulacyjne (świadek zmyślił oraz Tomek uderzył Krzysztofa) oraz dwie dezinformacje dysymulacyjne (świadek zataił oraz Krzysztof uderzył Tomka). W komunikatach wojennych wykorzystuje się ten rodzaj dezinformacji do podkreślenia, że nieprzyjaciel poniósł porażkę, mimo że odniósł on zwycięstwo.

Zakończenie

Podstawowym narzędziem komunikacji *inter vivos* jest informacja. Stanowi ona nośnik wielu danych. Dzięki niej możliwe jest funkcjonowanie wielu obszarów ludzkiego życia. Naukowcy z dziedziny cybernetyki spostrzegli, że ludzkość ma kłopot z określeniem i stworzeniem definicji pojęcia „informacja". Zadania stworzenia definicji podjął się Marian Mazur. Jego badania stworzyły podwaliny pod jakościową teorię informacji. Jej zadaniem było określić informację oraz przeprowadzić analizę i syntezę tej ważnej rzeczywistości. Ponadto uzewnętrzniła ona różnice pomiędzy doktryną a nauką. Nauka o informacji oraz jej teoria i jakość pokazały, że naukowcy chcą, żeby ich poglądy pasowały do rzeczywistości. Doktrynerzy potrzebują, żeby rzeczywistość pasowała do ich poglądów. Zadaniem naukowca jest poszukiwanie prawdy, dlatego martwią się trudnościami w jej znajdowaniu. Doktryner zna prawdę od początku i cieszy się jej zupełnością. Idąc dalej, naukowiec ma mnóstwo wątpliwości, czy jest prawdą to, co mówi nauka, a przedstawiciel doktryny nie ma wątpliwości, że

46 Ibidem.

jest prawdą to, co mówi doktryna. Naukowiec uważa, że to, co mówi nauka jest nietrwałe, dlatego doktryner twierdzi, że to, co mówi doktryna trwa wiecznie.

Powyższe studium pokazało, czym jest informacja oraz jak wygląda nauka o informacji. Ponadto przedstawiano jej podstawowy wymiar, wskazano jej operacyjny i zasadniczy charakter. Bardzo cenny opis stanowi analiza różnych obszarów życia ludzkiego, w którym występują różne rodzaje informacji, w tym pozorne i fałszywe. Ponieważ pseudoinformacja oraz dezinformacja występują bardzo często, dlatego w artykule dokonano ich charakterystyki i pokazano praktyczne zastosowanie.

Bibliografia

Brillouin L., *Science and Information Theory*, New York 1956.
Cherry C., *On human communication. A revive, a survey and criticism*, Massachusetts 1966.
Comfort A., *Biological Aspects of Senescence*, „Biological Reviews" 1954, nr 29.
Couffingal L., *La Cybernetique*, Paris 1963.
Czapliński L., *Księga przysłów, sentencji i wyrazów łacińskich*, reprint, Warszawa 1987.
Flechtner H.J., *Grundbegriffe der Kybernetik*, Stuttgart 1966.
Geppert M., *Uwagi o koncepcji dwóch systemów sygnałowych*, „Studia Filozoficzne" 1961, nr 4.
Jaspers K., *Problem winy*, Warszawa 2018.
Kalinowski S., *Scire Latine. Język łaciński. Podręcznik dla alumnów i studentów teologii*, Warszawa 2014.
Kiełpiński K., *Decepcja jako fundamentalne narzędzie pracy służb specjalnych w ramach wojny hybrydowej*, https://disinfodigest.pl/decepcja-jako-narzedzie-pracy-sluzb-specjalnych-w-ramach-wojny-hybrydowej/ [dostęp: 13.06.2022].
Kowalski A., *Kontra. Sztuka walki z wywiadem przeciwnika*, Łomianki 2021.
Krajczyński J., *Wystąpienia wiernych w mass mediach w sprawach wiary i obyczajów* [w:] *Fides, quae de verbo nascitur et nutritur. Nauczycielskie zadanie Kościoła wobec 1050 rocznicy chrztu Polski*, red. J. Krajczyński, A. Domaszk, Płock 2016.
Mazur M., *Cybernetyka a humanitaryzm*, „Argumenty za i przeciw" 1963, nr 4.
Mazur M., *Cybernetyka i charakter*, Warszawa 1976.
Mazur M., *Jakościowa teoria informacji*, Warszawa 1970.
Munkler H., *Wojny naszych czasów*, Kraków 2004.
Netzley M., Snow C., *Pisanie raportów*, Warszawa 2009.
Piasecki B., *Kontrwywiad, atak i obrona*, Łomianki 2021.
Shannon C., *A mathematical theory of communication*, „The Bell System Journal" 1948, nr 27.
Siuda P., Wasylczyk P., *Publikacje naukowe*, Warszawa 2018.
Śliwierski B., *Habilitacja: diagnoza – procedury – etyka – postulaty*, Kraków 2017.
Weiner N., *Cybernetics or control communication in the Animal and the Machine*, New York 1948.

Apparent and false information in qualitative information theory. Analysis in the area of cybernetics

Abstract

Information is the basic tool of *inter vivos* communication. It serves as a carrier for many data. Thanks to it, many areas of human life can function. Cybernetic scientists have recognized that mankind has difficulty defining and defining „information". Marian Mazur undertook the task of creating the definition. His research laid the groundwork for a qualitative information theory. Its task was to define the information and carry out the analysis and synthesis of this important reality. Moreover, it showed the differences between doctrine and science. Information science and its theory and quality have shown that scientists want their views to fit with reality. Doctrinaires need reality to match their views. The task of a scientist is to search for truth, therefore he is worried about the difficulties of finding it. The doctrinaire knows the truth from the beginning and enjoys its completeness. Moving on, the scientist has a lot of doubts that what the science says is true, while the representative of the doctrine has no doubt that what the doctrine says is true. After all, the scientist thinks what science says is impermanent, so the doctrine says what the doctrine says lasts forever.

The above study showed what information is and what the science of information looks like, moreover, its basic dimension was presented, indicating its operational and essential character. A very valuable description is the analysis of various areas of human life, in which there are various types of information, among them false and false. Pseudo-information and disinformation occur very often, therefore the next thought expressed in the article was the characteristics and their practical application.

Key words: information, apparent information, false information, qualitative theory, simulation, dissimulation, confusing nature of information

Anna Felkner*

Źródła użytecznych informacji o zagrożeniach w internecie rzeczy

Streszczenie

Jednym z wielu problemów, z jakimi borykają się użytkownicy, producenci czy właściciele sieci oraz osoby na co dzień zajmujące się cyberbezpieczeństwem, jak pracownicy zespołów CSIRT, jest kwestia podatności w urządzeniach internetu rzeczy. Mimo że najpopularniejsze podatności są często przedstawiane dużemu gronu odbiorców, nadal zdecydowana większość z nich jest znana tylko specjalistom od cyberbezpieczeństwa, a nie użytkownikom, którzy to podatne urządzenie mają. Dlatego to właśnie użytkownicy najczęściej mogą być zagrożeni. W związku z tym jest wskazane zwiększenie świadomości użytkowników zagrożeń płynących z posiadania i używania niezabezpieczonych urządzeń, a także zapewnienie dostępu do informacji o podatnościach. Idealnie byłoby mieć jedno źródło, w którym informacje o podatnościach i eksploitach związanych z urządzeniami IoT byłyby zebrane, zagregowane i skorelowane. Nasze obserwacje po analizach wskazały, że wciąż takiego zadowalającego źródła brakowało, dlatego też zdecydowaliśmy się stworzyć repozytorium, w którym informacje o podatnościach i eksploitach mogą być łatwo dostępne dla każdego. W artykule zostały przedstawione m.in. różne źródła użytecznych informacji (actionable information), a także otwarte repozytorium, które w przystępny sposób przedstawia informacje o podatnościach i eksploitach w internecie rzeczy.

Słowa kluczowe: internet rzeczy, IoT, podatność, eksploit, baza informacji o podatnościach i eksploitach, użyteczne informacje

* Anna Felkner, NASK, e-mail: anna.felkner@nask.pl.

Internet rzeczy to koncepcja połączonych ze sobą inteligentnych urządzeń. Koncepcja ta zyskuje coraz większą popularność i stała się rzeczywistością z udziałem każdego z nas. Urządzenia te oferują użytkownikom mnóstwo możliwości w zależności od ich potrzeb. Produkty, które można nazwać inteligentnymi, są ciągle rozwijane i dziś można tak nazwać nie tylko routery, kamery i czujniki bezprzewodowe, lecz także wszelkiego rodzaju inteligentne urządzenia domowe (odkurzacze, pralki, telewizory, lodówki), inteligentne samochody, urządzenia monitorujące zdrowie oraz różnorodne urządzenia przemysłowe – Industrial Control Systems (ICS) i Industrial Internet of Things (IIoT). Biorąc pod uwagę to, że urządzenia internetu rzeczy towarzyszą nam każdego dnia zarówno w życiu prywatnym, jak i zawodowym, zarówno w domu, jak i w przemyśle, zarówno w służbie zdrowia, jak i na ulicach nie możemy pominąć kwestii związanych z ich bezpieczeństwem. Obecny stan bezpieczeństwa urządzeń IoT jest na bardzo niskim poziomie. O ile świadomość w kontekście bezpieczeństwa IT jest stosunkowo wysoka, o tyle świadomość IoT jest wciąż w powijakach. Wielu producentów, często nieświadomie, zaniedbuje ten temat, dlatego że wcześniej nie mieli oni doświadczeń z cyberbezpieczeństwem. W ostatnim czasie, na szczęście, świadomość użytkowników tych urządzeń wzrasta, nadal jednak nie jest to temat w pełni zaspokojony.

Najczęstsze problemy związane z bezpieczeństwem IoT to te, które dotyczą dostępu i szyfrowania. Urządzenia IoT zazwyczaj nie były projektowane z uwzględnieniem bezpieczeństwa jako podstawowej koncepcji. Doprowadziło to do licznych naruszeń sieci domowych i firmowych. Ponadto, jeżeli atakujący ma zdalny dostęp do urządzenia IoT, to może uzyskać dostęp do innych urządzeń IoT w skompromitowanej sieci. Dlatego niezwykle ważna jest ocena zarówno bezpieczeństwa urządzenia, jak i reputacji bezpieczeństwa dostawcy podczas projektowania sieci urządzeń IoT. Jedną z możliwości zabezpieczenia swoich urządzeń IoT jest wdrożenie odrębnej sieci dla sprzętu IoT, odseparowanej i odizolowanej od sieci podstawowej. Drugim niezwykle istotnym aspektem jest aktualizowanie oprogramowania, ograniczanie dostępu fizycznego i logicznego, monitorowanie całej aktywności sieciowej oraz wdrażanie zapór sieciowych i filtrowania ruchu.

Posiadanie informacji o podatnościach (czyli wszelkiego rodzaju lukach w oprogramowaniu lub sprzęcie) i eksploitach (czyli określonym kodzie lub technice wykorzystującej podatność) urządzeń IoT ma kluczowe znaczenie z punktu widzenia właścicieli urządzeń, dostawców usług, właścicieli sieci i producentów urządzeń. Pozyskiwanie tych informacji jest również krytyczne z punktu widzenia krajowych i sektorowych zespołów CSIRT (Zespoły

Reagowania na Incydenty Bezpieczeństwa Komputerowego, Computer Security Incident Response Teams). Zarządzanie podatnościami jest jednym z głównych aspektów bezpieczeństwa zarówno w świecie IT, jak i IoT czy IIoT.

W artykule zostały wykorzystane wyniki badań prowadzonych w ramach projektu Vulnerability and Attack Repository for IoT (VARIoT)[1], w których brały udział następujące osoby: Anna Felkner, Marek Janiszewski, Piotr Lewandowski, Marcin Rytel i Hubert Romanowski. Celem projektu było dostarczenie użytecznych informacji o urządzeniach internetu rzeczy, które mogą być przetwarzane ręcznie lub automatycznie w celu zapewnienia cyberbezpieczeństwa tych urządzeń. W naszej pracy skupiliśmy się na poszukiwaniu informacji o eksploitach i podatnościach w internecie rzeczy i zauważyliśmy, że nie ma jednego źródła, które przedstawiałoby szeroki zakres informacji związanych z tym aspektem bezpieczeństwa. Z naszych badań wynikało, że chociaż informacje były dostępne online, nie było jednego serwisu oferującego dane dotyczące IoT, a samo znalezienie czy wyselekcjonowanie tych informacji nie było trywialne. Krajowe bazy danych o podatnościach zawierają pewne wpisy dotyczące IoT, ale brakuje w nich mechanizmów pozwalających na odróżnienie ich od innych podatności. Co więcej, informacje o wielu podatnościach dotyczących świata internetu rzeczy nigdy nie trafiają do tych baz, ale można je znaleźć rozproszone w internecie, dlatego postanowiliśmy stworzyć takie źródło.

Na początek przeanalizowaliśmy ponad 100 unikalnych źródeł różnego typu. Były to zarówno źródła ustrukturyzowane, które zawierają informacje nie tylko o IoT, lecz także, a raczej przede wszystkim, o ogólnym IT, różne krajowe bazy danych o podatnościach, a także źródła nieustrukturyzowane takie, jak: raporty, blogi czy indywidualne strony internetowe. Z analizy poszczególnych źródeł wynika, że nie istniała jedna, kompleksowa, przeznaczona dla IoT baza danych o podatnościach i eksploitach. Dostępne rozwiązania zostały stworzone z myślą o podatnościach w oprogramowaniu i sprzęcie głównie IT i nie są dobrze przystosowane do zarządzania podatnościami dotyczącymi świata IoT, w którym krzyżuje się wiele domen – sprzęt, oprogramowanie i sieci. Zwykle źródłem informacji o podatnościach są bazy danych o podatnościach. Najpopularniejszą z nich jest baza NVD (National Vulnerability Database)[2], która jest zsynchronizowana z listą CVE (Common Vulnerabilities

1 *Vulnerability and Attack Repository for IoT Project*, https://www.variot.eu [dostęp: 5.01.2023].

2 *National Vulnerability Database*, https://nvd.nist.gov/ [dostęp: 5.01.2023].

and Exposures)[3] i opisuje jedynie podatności z przypisanymi do nich wpisami CVE. Program Common Vulnerabilities and Exposures jest słownikiem zidentyfikowanych podatności. Lista ta pozwala zainteresowanym stronom uzyskać szczegółowe informacje o podatnościach poprzez odwołanie się do unikalnego identyfikatora znanego jako CVE ID. Większość z ogólnych baz podatności nie ma wbudowanej kategoryzacji, która pomogłaby wyselekcjonować z ich zbiorów podatności dotyczące urządzeń IoT. Dlatego wykorzystanie tych baz jako podstawowego źródła do automatycznego zbierania informacji wymaga wcześniejszej wiedzy o tym, które zasoby należą do świata IoT. Rynek urządzeń inteligentnych jest zróżnicowany i szybko rozwijający się, z dużą liczbą producentów, którzy oferują te same produkty pod różnymi markami i nazwami handlowymi. Trudno jest jasno zdefiniować, czym tak naprawdę jest IoT. Ponieważ nie ma jedynej słusznej definicji IoT, więc w naszej pracy przyjęliśmy jako urządzenie IoT określać każdy przedmiot (oprócz telefonu, komputera PC, tabletu i sprzętu centrum danych) wyposażony w łączność sieciową oraz zdolność do gromadzenia i wymiany danych. Wprawdzie smartfony są czasami uważane za urządzenia IoT, lecz zdecydowaliśmy się wyłączyć je z naszej definicji, dlatego że ich stale rosnące możliwości obliczeniowe spowodowały, że łatwiej jest je zaklasyfikować raczej jako komputery przenośne niż proste „rzeczy" podłączone do internetu.

Jak wspomniano wcześniej, istnieje wiele publicznie dostępnych baz danych zawierających różne informacje o podatnościach w różnych typach sprzętu i oprogramowania. Tylko kilka z nich jest poświęconych wyłącznie internetowi rzeczy lub przynajmniej w jakiś sposób wskazuje na takie podatności, ale żadna z nich nie agreguje bezpośrednio informacji z innych źródeł. Poniżej krótko opisano źródła, z których są pobierane dane. Wspomniane wyżej NVD[4] jest ogólną bazą danych o podatnościach prowadzoną przez National Institute of Standards and Technology (NIST). Analizuje i punktuje podatności, które mają nadany unikalny identyfikator CVE. Inną ogólną bazą danych o podatnościach jest China National Vulnerability Database (CNVD)[5] utrzymywana przez chiński krajowy CERT – National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC). Jest jedyną spośród narodowych baz podatności, która kategoryzuje podatności

3 *Common Vulnerabilities and Exposures*, https://cve.mitre.org/ [dostęp: 5.01.2023].
4 *National Vulnerability Database*, https://nvd.nist.gov/vuln/search [dostęp: 5.01.2023].
5 *Chinese National Vulnerability Database of Information Security*, http://www.cnnvd.org.cn/ [dostęp: 5.01.2023].

ze względu na rodzaj podatnego produktu i posiada kategorię przeznaczoną dla IoT. Chinese National Vulnerability Database of Information Security (CNNVD)[6] jest bazą podatności utrzymywaną przez chińską agencję rządową – China Information Technology Security Evaluation Center (CNITSEC). Japan Vulnerability Notes iPedia (JVNDB)[7] jest bazą danych o podatnościach prowadzoną przez JPCERT Coordination Center oraz Information-technology Promotion Agency (IPA)[8] z Japonii. Wpisy w bazie są napisane w języku japońskim, ale podzbiór jej danych jest również dostępny w języku angielskim. Baza ICS Vulnerability Database (IVD)[9], obecnie niedostępna, była prowadzona przez chińską firmę Winicssec Technologies i skupiała się wyłącznie na podatnościach występujących w przemysłowych systemach sterowania. Większość jej wpisów stanowiły informacje z NVD, CNVD i CNNVD. Chiński ICS CERT jest częścią CNCERT/CN, opiekuna opisanej wcześniej bazy CNVD. Prowadzi on własną listę podatności[10] skoncentrowaną głównie na podatnościach systemów ICS. Carnegie Mellon University's Software Engineering Institute CERT/CC[11] często publikuje informacje o nowo odkrytych podatnościach, z których część nie znajduje się w NVD. Inne zespoły CERT rzadko zamieszczają na swoich stronach internetowych informacje o podatnościach. Jeżeli nawet są one prezentowane, to podatności dotyczące urządzeń IoT są rzadko spotykane i brakuje ich kategoryzacji. Vulmon jest wyszukiwarką podatności w zabezpieczeniach z bardzo prostym interfejsem[12]. Zero Day Initiative (ZDI) to międzynarodowa inicjatywa prowadzona przez firmę Trend Micro Inc. zajmującą się cyberbezpieczeństwem[13]. Zero Day Initiative odkupuje znalezione podatności od niezależnych badaczy bezpieczeństwa, po czym ujawnia je producentom w celu załatania ich przed upublicznieniem informacji. Zero Science Lab (ZSL) to macedońskie laboratorium badawczo-rozwojowe zajmujące się bezpieczeństwem informacji[14]. Oprócz podatności pozyskujemy też infor-

6 *China National Vulnerability Database*, https://www.cnvd.org.cn/ [dostęp: 5.01.2023].
7 *Japan Vulnerabilities Notes Database*, https://jvndb.jvn.jp/en/ [dostęp: 5.01.2023].
8 *Information-technology Promotion Agency*, https://www.ipa.go.jp/english/ [dostęp: 5.01.2023].
9 *ICS Vulnerability Database*, http://ivd.winicssec.com/ [dostęp: 5.01.2023].
10 *Chinese ICS-CERT website*, https://www.ics-cert.org.cn/portal/index.html [dostęp: 5.01.2023].
11 *Carnegie Mellon University CERT Coordination Center*, https://www.kb.cert.org/vuls/ [dostęp: 5.01.2023].
12 *Vulmon Vulnerability Search Engine*, https://vulmon.com/ [dostęp: 5.01.2023].
13 *Zero Day Initiative*, https://www.zerodayinitiative.com/ [dostęp: 5.01.2023].
14 *Zero Science Lab*, https://www.zeroscience.mk/en/index.php [dostęp: 5.01.2023].

macje o eksploitach z różnych źródeł, m.in. z Exploit DB[15] czy Packet Storm[16]. Źródła zostały dokładniej opisane w pracy Marcina Rytla, Anny Felkner i Marka Janiszewskiego[17].

W artykule przeanalizowano jedynie publicznie dostępne darmowe źródła informacji, co wyklucza płatne serwisy takie, jak m.in. agregator podatności i eksploitów Vulners[18]. Vulners to serwis agregujący informacje dotyczące cyberbezpieczeństwa z wielu źródeł, począwszy od baz danych o podatnościach i ekploitach, poprzez poradniki bezpieczeństwa producentów, aż po blogi związane z bezpieczeństwem. Obecnie dostępne są dane ze 191 źródeł, w tym z niektórych opisanych wcześniej: CNVD, NVD, JVNDB czy ZDI. Jakość i kompletność danych jest różna – często w danych Vulners brakuje części informacji znajdujących się w oryginalnym źródle dla poszczególnych wpisów lub nie wszystkie wpisy z danego źródła są dostępne w Vulners.

Tabela 1. Spis źródeł informacji o podatnościach i eksploitach

Skrót	Nazwa	Typ bazy
CERT CC	Carnegie Mellon University CERT Coordination Center	podatności
CNNVD	Chinese National Database of Information Security	podatności
CNVD	China National Vulnerability Database	podatności
Exploit-DB	Exploit Database by Offensive Security	eksploity
ICS-CERT CN	Chinese ICS-CERT website	podatności
IVD	ICS Vulnerability Database	podatności
JVNDB	Japan Vulnerabilities Notes Database	podatności
NVD	National Vulnerability Database	podatności
Packet Storm	Packet Storm Security	podatności/eksploity
Vulmon	Vulmon Vulnerability Search Engine Vulnerability	podatności
ZDI	Zero Day Initiative	podatności
ZSL	Zero Science Lab	podatności

Ponieważ wiele podatności i eksploitów dotykających urządzenia IoT nigdy nie zostaje skatalogowane w bazach danych, więc jest konieczne przeglądanie dodatkowych źródeł, żeby zachować świadomość krajobrazu zagrożeń

15 *Offensive Security's Exploit Database Archive*, https://www.exploit-db.com/ [dostęp: 5.01.2023].

16 *Packet Storm*, https://packetstormsecurity.com/ [dostęp: 5.01.2023].

17 M. Rytel, A. Felkner, M. Janiszewski, *Towards a Safer Internet of Things – A Survey of IoT Vulnerability Data Sources*, „Sensors" 2020, t. 20, nr 21.

18 *Vulners – Vulnerability Database*, https://vulners.com/ [dostęp: 5.01.2023].

IoT. Oprócz wpisów zebranych ze źródeł ustrukturyzowanych wymienionych w tabeli 1 szukaliśmy również najnowszych postów i artykułów pojawiających się w internecie. Dobrym źródłem są blogi, ale trudno je śledzić i wyciągać z nich istotne informacje. Są one pisane przez indywidualnych badaczy, grupy hakerskie lub firmy zajmujące się bezpieczeństwem, prezentujących swoje osiągnięcia w hakowaniu inteligentnych urządzeń. Ponieważ rzadko są one poświęcone wyłącznie temu tematowi, więc poszczególne posty związane z IoT trzeba filtrować. W przypadku tego rodzaju źródeł odpowiednie metadane można wyodrębnić z surowego tekstu. Jedną z unikalnych cech zbudowanej bazy podatności VARIoT jest korelacja i agregacja informacji o podatnościach z różnych publicznie dostępnych źródeł.

Cały proces tworzenia bazy podatności i eksploitów IoT, którą przygotowaliśmy w trakcie realizacji projektu VARIoT (zob. rys. 1), można przedstawić w kilku fazach. W pierwszej została przeprowadzona identyfikacja i selekcja wartościowych źródeł informacji związanych z podatnościami i eksploitami. Przedmiotem zainteresowania są tu zarówno ustrukturyzowane źródła (z których łatwiej jest pobrać dane), jak i nieustrukturyzowane, takie jak blogi czy indywidualne strony internetowe (z których pobieranie danych jest zwykle bardziej skomplikowane, ale mogą one dostarczać informacji wyprzedzających oficjalne bazy danych lub zawierać zupełnie unikalne dane). W drugim etapie zbieraliśmy informacje z tych źródeł, w trzecim informacje te były standaryzowane, w czwartym – informacje z różnych źródeł na temat danej podatności lub eksploita były korelowane i agregowane. Piąty polega na wzbogaceniu i wyborze najbardziej wiarygodnych informacji o każdej podatności i eksploicie. Na podstawie informacji zawartych w bazie danych oraz uzyskanych od konsorcjantów projektu VARIoT przygotowaliśmy słowniki informacji o producentach, modelach i typach urządzeń oraz o typach podatności. Słowniki te zostały wykorzystane jako słowa kluczowe do wyszukiwania w tekście oraz jako zbiory danych treningowych dla innych metod. Ocena zaufania ma na celu wybór najbardziej wiarygodnej i informacyjnej części informacji, ocenę wiarygodności informacji oraz identyfikację podatności i eksploitów związanych z IoT. Odbywa się to na podstawie reputacji źródła, zbieżności informacji z różnych źródeł, metody agregacji i klasyfikacji oraz dodatkowych wyszukiwań. Stworzona w opisany powyżej sposób baza danych może być następnie udostępniana i wykorzystywana przez różne podmioty do różnych celów. Wyszukiwanie informacji związanych z IoT odbywa się również poprzez filtrowanie na różnych

poziomach z wykorzystaniem stworzonej przez nas taksonomii urządzeń IoT, wewnętrznego katalogu urządzeń IoT, mechanizmu filtrowania na podstawie słów kluczowych itp.[19].

Źródło: NASK-PIB.

Rys. 1. Sposób tworzenia bazy danych podatności

Stworzenie uporządkowanej, publicznie dostępnej bazy danych zawierającej informacje o znanych podatnościach technicznych i eksploitach jest niezwykle korzystne dla wszystkich interesariuszy: użytkowników, producentów i właścicieli sieci, a także zespołów CSIRT czy innych osób zajmujących się bezpieczeństwem urządzeń i oprogramowania. Zbadaliśmy duży przekrój różnego rodzaju źródeł i na tej podstawie możemy stwierdzić, że zbierając dane z wielu źródeł, możemy uzyskać bardziej kompletny i wyczerpujący wpis na temat danej luki lub eksploita niż z jednego źródła. Ponieważ przeszukujemy wiele różnych typów publicznie dostępnych źródeł, a nasza baza danych koreluje i agreguje dane z tych źródeł, więc sprawia to, że każdy wpis jest bogaty

19 Szczegółowy opis etapów zob. M. Janiszewski, A. Felkner, P. Lewandowski, M. Rytel, H. Romanowski, *Automatic Actionable Information Processing and Trust Management towards Safer Internet of Things*, „Sensors" 2021, t. 21, nr 13.

w informacje, które mogą być wykorzystane do zapewnienia bezpieczeństwa urządzeń IoT, a także zmniejsza ryzyko pominięcia niektórych danych lub opóźnień w uzyskaniu informacji o konkretnych podatnościach.

Stworzona przez nas baza informacji o podatnościach i eksploitach IoT została opublikowana na stronie https://www.variotdbs.pl/. Strona dostępna jest w dwóch językach (angielskim i polskim), a szczegółowe informacje dotyczące podatności i eksploitów dostępne są tylko w języku angielskim. Główne sekcje, które można znaleźć na stronie, to:

1) podatności – tutaj przedstawione są luki bezpieczeństwa dotykające urządzeń IoT. Sekcja ta umożliwia przeglądanie najnowszych podatności IoT oraz ich wyszukiwanie. Wyszukiwanie podatności jest możliwe z wykorzystaniem atrybutów zarówno według producenta, modelu urządzenia i jego wersji, identyfikatora CVE, identyfikatora VARIoT, numeru CWE (Common Weakness Enumeration[20]) oraz typu, jak i dowolnej frazy opisującej podatność. Takie wyszukiwanie daje wiele możliwości, dlatego że można znaleźć opis podatności, wykorzystując dowolne z powyższych pól, np. typ urządzenia, oraz inne powiązane źródła informacji o podatnościach. Każdy wpis składa się z danych dotyczących konkretnej podatności znalezionych z różnych źródeł, zawiera źródła informacji i obliczone poziomy zaufania, a także zagregowane linki do zewnętrznych źródeł, z którymi można zapoznać się w celu uzyskania dalszych informacji;

2) eksploity – tutaj prezentowane są publicznie dostępne eksploity wymierzone w urządzenia IoT. Sekcja ta pozwala na przeglądanie eksploitów, które mogą zagrażać urządzeniom IoT. Działa ona w podobny sposób jak sekcja „podatności", czyli też można szukać informacji o eksploitach według producenta, modelu czy wersji urządzenia;

3) wiadomości – tutaj można zobaczyć automatycznie generowaną listę wiadomości na temat bezpieczeństwa IoT, które to wiadomości zostały zebrane przy użyciu wyszukiwarki wykorzystującej autorskie skrypty do filtrowania wyników wyszukiwania. Sekcja ta pokazuje różnego rodzaju informacje związane z podatnościami w świecie internetu rzeczy. Wiadomości są zbierane z różnych źródeł, głównie nieustrukturyzowanych, takich, jak: raporty, blogi, informacje dostarczane przez osoby zajmujące się badaniem podatności lub w jakikolwiek sposób związane z cyberbezpieczeństwem.

20 *Common Weakness Enumeration*, https://cwe.mitre.org/ [dostęp: 5.01.2023].

4) API – tutaj znajduje się opis jak w prosty sposób pobrać dane, które udostępniamy na stronie poprzez API. Można to zrobić za pomocą jednego z dwóch formatów plików, tj. JSON i JSON-LD;

5) ontologia – tutaj znajduje się opis ontologii wpisów do baz podatności i eksploitów VARIoT (tylko w języku angielskim).

Bazy danych podatności i eksploitów budowane są na podstawie wcześniej opisanych źródeł. Wyszukiwarka wiadomości korzysta z wielu dostępnych wyszukiwarek internetowych i na podstawie znalezionych w ten sposób informacji tworzy wpis przedstawiający dodatkowe informacje o podatnościach i urządzeniach, które pozyskiwane są za pomocą przetwarzania języka naturalnego (Natural Language Processing – NLP), uczenia maszynowego (Machine Learning – ML) i sztucznej inteligencji (Artificial Intelligence – AI) oraz specjalnie do tego przygotowanych filtrów w celu lepszego dostosowania wpisu i połączenia danych uzyskanych z wielu źródeł. Opracowany mechanizm jest w stanie wydobyć informacje z nieustrukturyzowanych źródeł informacji takich, jak: blogi, raporty i artykuły. Ponadto oblicza zaufanie do wybranych informacji, żeby lepiej ocenić ich istotność. W kontekście bazy danych podatności i eksploitów zaufanie opiera się na punktacji wiarygodności źródeł ustalonej na podstawie naszej wiedzy o tych źródłach, a w kontekście wiadomości – na informacjach wyodrębnionych ze znalezionych wpisów, tj. słowa kluczowe, nazwy producentów i produktów, typy podatności oraz linki do znanych baz danych podatności[21].

Wraz z gwałtownym wzrostem wykorzystania produktów IoT w różnorodnych zastosowaniach ich bezpieczeństwo staje się coraz większym problemem. Duża liczba podatności w zabezpieczeniach w połączeniu z brakiem wystarczającego wsparcia dla produktów i procesów łatania zagraża gospodarce, bezpieczeństwu obywateli i ich prywatności. Niezabezpieczone urządzenia IoT już teraz są wykorzystywane w masowych atakach, które mogą stać się jeszcze większe i częstsze, jeżeli nie zostaną podjęte działania mające na celu zabezpieczenie środowiska IoT. Publicznie dostępne źródło uporządkowanych informacji o znanych podatnościach i eksploitach w urządzeniach IoT to wielki krok w kierunku poprawy bezpieczeństwa tych urządzeń. Jak dotąd, żadne z istniejących rozwiązań nie było zadowalające, co podkreślało potrzebę stworzenia bazy danych skoncentrowanej na IoT. Przygotowane przez nas

21 Więcej na ten temat zob. A. Felkner, M. Rytel, *A Repository of Actionable Information on the Internet of Things* [w:] *Proceedings of the 19th International Conference on Wireless Networks and Mobile Systems*, t. 1, [Lizbona] 2022, s. 69–75.

repozytorium jest publicznie dostępne na poświęconej jej stronie[22], za pośrednictwem Europejskiego Portalu Danych[23] oraz krajowych Portali Danych (jak polski Portal Otwartych Danych[24]), a także innych źródeł, jak Malware Information Sharing Platform (MISP), która jest powszechnie wykorzystywana przez społeczność analityków cyberbezpieczeństwa oraz za pośrednictwem sieci dystrybucji organizacji ShadowServer, dzięki której dane są raportowane do krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego i zweryfikowanych właścicieli sieci.

Bibliografia

Felkner A., Rytel M., *A Repository of Actionable Information on the Internet of Things* [w:] *Proceedings of the 19th International Conference on Wireless Networks and Mobile Systems*, t. 1, [Lizbona] 2022.

Janiszewski M., Felkner A., Lewandowski P., Rytel M., Romanowski H., *Automatic Actionable Information Processing and Trust Management towards Safer Internet of Things*, „Sensors" 2021, t. 21, nr 13.

Rytel M., Felkner A., Janiszewski M., *Towards a Safer Internet of Things — A Survey of IoT Vulnerability Data Sources*, „Sensors" 2020, t. 20, nr 21

Sources of actionable information about threats on the Internet of Things

Abstract

One of the many problems facied by users, producers or network owners as well as those who deal with cybersecurity on a daily basis is the issue of vulnerabilities in Internet of Things devices. Although the most popular vulnerabilities are often presented to the general public, the vast majority of them are still known only to cybersecurity specialists, and not to the users who own the vulnerable device. Consequently, it is the users who are most likely to be at risk. It is advisable to increase user awareness of the dangers of owning and using unsecured devices as well as provide access to information about vulnerabilities. Ideally, we would like to have a single source where information about vulnerabilities and exploits related to IoT devices would be collected, aggregated and correlated. Among other things, the article presents various sources of actionable information as well as an open repository that presents information about vulnerabilities and exploits in an accessible way.

Key words: Internet of Things, IoT, vulnerability, exploit, vulnerability and exploit database, actionable information

22 *VARIoT baza podatności i eksploitów IoT*, https://www.variotdbs.pl/ [dostęp: 5.01.2023].
23 https://data.europa.eu.
24 https://dane.gov.pl/.

Tomasz Mielko*

Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel

Abstract

The subject of this article is a discussion of the legal provisions governing the Israeli and international legal systems governing the control of trade in cyber-surveillance tools. A detailed analysis of the current regulations is carried out with a view to classification and pointing out imperfections in the content of the current regulations. The author identifies the transformations in the content of the Wassenaar Arrangement, which resulted in an attempt to regulate this matter more comprehensively in Israeli law in 2016. Using the impact of the international NSO software scandal as an example, the role that an effective export control regime, including international regulation, plays in preventing cyber-surveillance tools from being used in ways that are dangerous to internationally recognized values is demonstrated.

Key words: cyber-surveillance, export control, Wassenaar Arrangement, cyber defence

* Tomasz Mielko is a lawyer in Miller Canfield global law firm. He specializes in defense and security matters, export controls, and public procurement law, e-mail: t.mielko@wp.pl, ORCID: 0000-0002-4863-6230.

For many years, with successive discoveries and technological advances, questions have been raised about the need to restrict access to effective and dangerous cyber tools against certain states as well as private actors who may use such tools to disrupt international peace and security, violate human rights or achieve goals politically and militarily contrary to the interests of the producer country. The problem is multidimensional, as the recent global espionage scandal involving the flagship software of the Israeli manufacturer NSO Group, the Pegasus system, vividly demonstrates. The scale of the excitement generated by the 2021 revelations of attacks using this system on journalists, opposition figures, lawyers, human rights activists, and the wider political opposition in many countries around the world, has completely obscured the important issue of controlling the proliferation of cyber surveillance systems and has not sufficiently prompted a discussion of the political and legal measures that should be implemented in the future to ensure that offensive cyber tools are used as a last resort, in a manner that is appropriate and fit for purpose.

This paper will discuss the internal and international legal regime under which the export of Israeli-made offensive cyber-surveillance tools, including the software known as the Pegasus system, takes place, taking into account developments in legislation covering Israeli export controls. This text will also focus on demonstrating the role that an effective export control system, including international regulations, plays in preventing the use of cyber surveillance tools in ways that are dangerous to internationally recognized values.

The current growing rivalry between major powers and the changes in the world order resulting from the transition to a multilateral order are resulting in an exponential demand by states for effective means of conducting offensive as well as defensive operations in a new war space – the cyber domain. This sphere, as was the case at the beginning of the 20th century with the advent of military aviation, is not yet fully regulated in international law, although noteworthy efforts are being made to produce universally applicable rules for the use of cyber weapons, or to interpret the law already in force in this area[1]. For the time being, the boundary between a state of war and peace in

1 Noteworthy documents include: M. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017; *The future of discussions on ICTs and cyberspace at the UN*, 10.08.2020, https://tiny.pl/95bk8 [access: 20.09.2022]. It should be noted that the UN Group of Governmental Experts on the Development of Responsible State Behaviour in Cyberspace in the Context of International Security was established, https://tiny.pl/95b29 [access: 20.09.2022].

the cyber domain is not yet clear, nor is it fostered by the attitude of many actors in the international arena, who are not interested in drawing a thin red line that would unambiguously allow these states to be separated from each other. Such trends are undoubtedly influencing the development of a huge cyber defense market in Israel[2].

A number of regional factors are also noteworthy, such as the continuing sense of insecurity for the state of Israel, the strong emphasis on private sector-state cooperation, the opening of offices of multinational corporations such as Oracle, Dell, IBM and Deutsche Telekom within the Advanced Technology Park, along with research and development centers. Israel also attaches great importance to the study of cyber-security, classes in this subject are taught in schools, and universities and the state also offers the possibility of obtaining a PhD in this field. Extremely interestingly, it is one of the few countries that uses its own armed forces as an incubator for the development of start-ups. High-quality professionals trained in military centers go into business after completing their service, combining business with the benefit of state security. Given the factors presented, enabling Israel to be counted as a powerhouse in terms of capabilities in the cyber domain, it is clear that the country is making an effort to support its own entrepreneurs in the ever-growing global cyber defence market[3]. The implications of the close link between this highly sensitive industry and the institutions and key interests of the state are extremely momentous[4].

Controlling the export of cyber surveillance products in Israel encounters severe restrictions, which are to some extent market-driven – cyber defence entrepreneurs are not interested in imposing additional restrictions and obligations on them, having the effect of limiting potential markets only to countries that guarantee an adequate level of respect for civil rights and freedoms. Another issue remains the political decisions of the Israeli government in this highly sensitive area, as selling, or refusing to sell, or even withholding access to software at the time of special operations can be part

2 S. Shulman, *As cyber wars escalates Israeli tech gains an edge*', CTech, 2.04.2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3902572,00.html [access: 21.09.2022].

3 J. Vadakkanmarveettil, *Why the Israelis lead the world in cyber security expertise*, Jigsawacademy, 27.01.2020, https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/ [access: 21.09.2022].

4 L. Tabansky, I. Ben Israel, *Cybersecurity in Israel*, New York 2015.

of the shaping of international relations, including political pressure on the entities to which such software has been offered.

In approaching the international legal regulations relating to export controls in Israel, it is important to point to binding international treaties relating to arms trade controls, among them: The Nuclear Non-Proliferation Treaty (NPT), the Biological Weapons Convention (BWC), the Chemical Weapons Convention (CWC), the Arms Trade Treaty (ATT), or the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW), and non-binding multilateral export control agreements such as the Australia Group (AG), the Nuclear Suppliers Group (NSG), the Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement.

It is important to point out that only the Wassenaar Arrangement[5] refers to export control mechanisms for cyber-surveillance technologies, and that control regulations for such technologies were introduced in December 2013[6]. This amendment, by adding two categories to the control list, now includes „intrusion software" and certain „IP network communications surveillance systems or equipment", these categories having been introduced in sections 4.A.5 and 5.A.1.j) respectively.

By definition „intrusion software" is software specifically designed or modified to evade detection by monitoring tools or to defeat the protective countermeasures of a network-capable computer or device, and meeting any of the following criteria: a. extracting data or information from, or modifying system or user data in, a network-capable computer or device; or b. modifying a standard execution path of a program or process to enable the execution of externally supplied instructions. In contrast, „IP network communications surveillance systems or equipment, and specially designed components therefor", having all of the following: 1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone): a. Analysis at the application layer [e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1)]; b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and c. Indexing of extracted data; and 2. Being specially designed to carry out all of the following:

5 Full text in English is available at https://www.wassenaar.org/control-lists/ [access: 21.09.2021].

6 I. Pyetranker, *An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement*, „Northwestern Journal of Technology and Intellectual Property" 2015, vol. 13/2, no. 3, p. 152–180.

a. Execution of searches on the basis of „hard selectors"; and b. Mapping of the relational network of an individual or of a group of people. 5.A.1.j. does not apply to systems or equipment, specially designed for any of the following: a. Marketing purpose; b. Network Quality of Service (QoS); or c. Quality of Experience (QoE).

Separately, the Wassenaar Arrangement also refers to cyber systems with strictly military applications, which are defined in the Munitions List under category ML.21.b.5. As proposed in the text of the Agreement, the definition of the indicated category is software specifically designed or modified for military offensive cyber operations. In addition, it is indicated that ML21.b.5. includes software designed to destroy, damage, degrade or disrupt systems, equipment or software as defined in the Munitions List, Cyber Reconnaissance and Cyber Command and Control. ML21.b.5. does not apply to vulnerability disclosure or cyber incident response limited to non-military defence preparedness or cyber security response. Given the nature of the software as defined in ML21.b.5 of the Wassenaar Arrangement Weapons List, it should be considered that the NSO Group's product does not fall within this type of software, as it is, according to the available information, designed to covertly infect the recipient's device, mainly a phone, and the software does not have the kinetic effects characteristic of the products defined in provision ML21.b.5 of the Weapons List. In classifying the Pegasus software produced by the NSO Group, it should be pointed out that, in light of the Wassenaar Arrangement, only software specifically designed, or modified, to generate, command and control or deliver „intrusion software" is on the Dual-Use List, as indicated in para. 4.D.4. Thus, Pegasus software, in the light of the Wassenaar Arrangement, does not fall into the category of armaments, nor does it fall into any category of dual-use items. Nevertheless, from a technical point of view, it is undisputed that the Pegasus software itself also requires equipment and technology to retrieve data from infected devices, possibly also to process the retrieved data and technical support equipment. Given the wording of the Wassenaar Arrangement regulations, the Pegasus system may require authorization as a dual-use product to the extent that Category 4.D.4. specifies that software and devices that are complementary within the Pegasus system infrastructure require authorization.

In view of the findings already made, it should be pointed out that the lists contained in the Wassenaar Arrangement, being non-binding, require implementation into the national legal order of the signatory states. This is most often done by extending the lists of dual-use items or weapon lists

in the legislation of the country concerned with the new categories adopted under the Arrangement. The specific legal language of the Arrangement has resulted in official guides being published in many countries around the world to enable exporters to verify whether their product falls under the export control regulations[7].

The legal regime adopted in Israel in this regard is unique. Although the country is not formally a member of the Wassenaar Arrangement, domestic legislation, the Defence Export Control Law (DECL)[8], directly references the Wassenaar Arrangement's list of arms and dual-use goods and technologies, with the exception of information security technologies (encryption devices). Israel is therefore treated as a compliant state, which is significant given that arms sales from Israel place the country among the top ten global exporters of such products. In addition to this, the DECL law authorised the Knesset to enact a national systematic list of arms and dual-use items, in accordance with the Annex to the Defence Export Control Regulation[9]. The body responsible for issuing export licences is the Defence Export Control Agency (DECA) within the Israeli Ministry of Defence, which issues licences for various defence-related goods and technologies, as well as dual-use items for national security purposes. Controlling the export of dual-use items for civilian end-users is the responsibility of the Israeli Ministry of Economy, which additionally also issues licences for the export of items related to sensitive goods and technologies: chemical, biological and nuclear, in addition, this body controls the export of Unmanned Aerial Vehicles and many other listed items. The export of cryptographic equipment is the responsibility of an autonomous unit of the Encryption Control Department at DECA[10]. Cryptographic assets are subject to a different legal regime, and the export control unit has overall oversight of cryptography issues, including responsibility for research and development of encryption techniques and devices. Israel applies a relatively simplified

7 An example is the guidance issued by the US Bureau of Industry and Security – https://www.bis.doc.gov/index.php/guidance [access: 21.09.2022].

8 Defense Export Control Law (Journal of Laws 2007, 5777 no. 274, p. 186) as amended, https://www.nevo.co.il/law_html/law01/999_796.htm [access: 21.09.2022].

9 Annex to the Defense Export Control Order, Combat Equipment & Controlled Dual-Use Equipment. KT 5640 no. 6640 of 1/13/2008, p. 348, https://www.nevo.co.il/law_html/law01/999_890.htm [access: 21.09.2022].

10 For more information on the jurisdiction of export control authorities in Israel: N. Margolis, *Work in progress? Israeli export control regulators face up to new challenges*, „WorldECR" 2021, issue 102, p. 28–30.

system of sanctions and embargoes, which is overseen by the Israeli Ministry of Finance.

The amendment of the Wassenaar Arrangement at the end of 2013 took the cyber market in Israel by surprise because, unlike in most countries, the Arrangement is directly binding in Israel and triggered by law the effect of having to place cyber-surveillance tools under export controls. At the same time, work was underway in the Israeli Ministry of Defence to comprehensively regulate the export control of products falling into the categories of „intrusion software" and „IP network communications surveillance systems or device", as part of internal regulations implementing and detailing the content of the provisions of the Wassenaar Arrangement in question.

In early 2016, a draft act emerged that established a broad regulatory framework for the export of cyber products[11]. This draft law included much broader export controls than is the case under the Wassenaar Arrangement standards, including to the extent that the Arrangement (section 4.D.4) does not include controls on products or devices on which software is run or stored[12]. The Israeli Defence Ministry also proposed to extend the definition of „intrusion software" to include certain products that can cause disruption to systems or any physical damage to a system. The draft regulation also included controls on the export (transmission) of exploits, cyber tools related to the military sphere and espionage and digital forensics devices. However, the important and, in retrospect, expedient draft was rejected, due to the highly critical stance taken by representatives of the Israeli cyber-military-industrial complex. Noteworthy for the arguments raised, industry representatives feared that the proposed regulation would restrict market access, lead to an exodus of talented professionals, reduce the competitiveness of Israeli companies in the industry, and consequently stagnate the dynamics of the rapidly growing cyber defence market, in which Israel is a global powerhouse. In the end, in the face of unified opposition from the industry, the draft regulation was rejected, leaving cyber surveillance software exporters with the possibility

11 D. Hindin, *Can Export Controls Tame Cyber Technology?: An Israeli Approach*, Lawfare, 12.02.2016, https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach [access: 21.09.2022].

12 A. Iliescu, *Israeli import, export, cyber regulation & enforcement*, Shibolet law, 19.05.2020, https://www.shibolet.com/en/israeli-import-export-and-cyber-regulation-and-enforcement/ [access: 21.09.2022].

of obtaining exemptions from the need to obtain export licences[13]. Given the extreme importance of the cyber industry and its close connection to state security interests, there was a tendency in Israel to deregulate and streamline as much as possible the export licensing process for cyber surveillance and cyber security tools.

Consequently, given that Israeli export control regulations do not restrict the export of cyber-surveillance tools due to the requirement to respect human rights in a particular country – offensive cyber surveillance tools have been sold to many countries around the world where standards of protection of human rights and fundamental freedoms are not guaranteed at a sufficiently high level. Although the activities of the NSO Group described above have been widely criticised, it must be recognised that the export of cyber surveillance tools by Israeli companies has complied with both national law and the Waasenaar Agreement, and therefore arguments sometimes made about the sale of cyberweapons to non-democratic countries should be regarded as unjustified under current law. Nevertheless, the DECL regulations, which do not in any way refer to the condition of respecting human rights in the country to which the export is made, should be regarded as a sham because, as a consequence, the adopted model, although formally allowing exporters to act within the limits of national and international law – violated the non formally binding standards of the international community.

In 2019 NSO Group reported that it has implemented an extensive compliance program internally to implement the principles of the UN Guiding Principles on Business and Human Rights. The company also has policies in place to protect human rights. The purpose of the 2019 – originated program is to address human rights violations within the business, and the controls used to achieve this are multi-stage. The primary tools used for compliance screening are due diligence and risk analysis, both in terms of customers and the category of product sold. The decision to sell a product is taken by a special committee chaired by the NSO President, the company's board of directors has the right to object in this respect. If the manufacturer receives information about an incident of infringement, the manufacturer proceeds to investigate the incident. If the information about the use of the software contrary to the contract or local law is confirmed – the manufacturer may terminate the

13 Y. Azulai, *Natanjahu scraps plans to regulate cybersecurity*, Globes, 19.04.2016, https://en.globes.co.il/en/article-netanyahu-scraps-plans-to-regulate-cyber-security-cos-1001118937 [access: 21.09.2022].

user's access to the software. In January 2021 NSO published its first ever „Transparency and Accountability Report", in which it reported extensively on the measures taken to protect human rights[14].

In November 2021, in response to incoming reports of NSO software being used against US security interests – the US Department of Commerce blacklisted the manufacturer of Pegasus, resulting in a ban on any US companies selling technology to NSO Group and its subsidiaries, at the same time Shalev Hulio, founder and CEO of NSO Group resigned to continue in office[15]. On 6 December 2021 DECA issued a statement announcing that the number of countries to which cyberweapons can be exported has been reduced from 102 to 37[16], in addition, the content of the end-user declaration has changed. Now, any contractor of Israeli companies exporting cyber-surveillance tools commits to using offensive cyber surveillance software only for counter-terrorism and combating serious crimes. Breach of the commitment results in the loss of the licence, including the exclusion of the software in the course of the mission, which undoubtedly constitutes a severe sanction for the purchaser's beneficial secret services.

The past year has been an exceptionally eventful and dynamic one for the cyber defence industry, and it seems that the series of major international scandals caused by NSO Group and its flagship software will serve as a warning to other cyber-surveillance tool makers. Not so long ago, NSO was at the center of French investor interest, only to find itself in dire financial straits a year later, lose its founder and be placed on the US Department of Commerce's sanctions list. Given the dynamic and continuous growth of the market for cyber-surveillance tools, as well as the fusion of cyber interests with the existential interests of rival states, as highlighted here on several occasions, there is no need to be optimistic about a moratorium on cyber weapons, or even more control over their proliferation. Export control regulations on their own may prove to be an insufficient measure to prevent advanced cyber-surveillance tools from being misused for their official purpose, but

14 *Transparency and Accountability Report 2021*, https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [access: 22.09.2022].

15 K. Huang, *Chief of Israeli Spyware Firm NSO to Step Down as It Revamps*, New York Times, 21.08.2021, https://www.nytimes.com/2022/08/21/business/nso-chief-executive-spyware.html [access: 22.09.2022].

16 Ch. Forrester, *Israel tightens regulations around cyber exports*, Janes.com, 7.12.2021, https://www.janes.com/defence-news/news-detail/israel-tightens-regulations-around-cyber-exports [access: 22.09.2022].

it is no less important to recognise that a milestone in this regard is the introduction of the new Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. New export control regulations for cyber-surveillance tools have also come into force in the United States, with new items added to the CCL list as of 19 January 2022 and additional definitions added to The Export Administration Regulations (EAR)[17]. The proposed changes aim to prohibit the sale of offensive cyber surveillance tools to authoritarian countries, including Russia and China.

The extremely interesting yet controversial example of the indirect influence of the interests of NSOs and similar companies on the content of export control regulation in Israel shows that leaving cyber-surveillance tools essentially out of effective control within the controlled trade is a profitable solution only in the very short term. There are many indications that the Israelis, who have so far led the way in developing cyber-surveillance tools, will be forced to give way to competitors who are far better able to exercise discretion around their activities without leading to their systems being used in a way that is widely objectionable. The political background to the decision to restrict the limit of countries to which exports of cyber surveillance tools from Israeli manufacturers are possible is also indicated by media reports of a significant reduction in the issuing of export licences and thus „starving the industry"[18]. It remains to be believed that Pegasus Gate will have a strong impact on the manufacturers of offensive cyber surveillance tools and that it will bring about the implementation of corporate mechanisms that will prevent scandals and thus the use of such tools will only be allowed as a last resort and against real threats to the functioning of democratic states.

17 Read more about the NSO acquisition plans *France and Israel hold 'secret' talks to defuse phone spyware row*, The Guardian, 22.10.2021, https://www.theguardian.com/world/2021/oct/22/france-and-israel-hold-secret-talks-to-defuse-phone-spyware-row [access: 23.09.2022].

18 The current state of the industry for cyber surveillance is described in an article A. Gilead, *Export controls strangling Israel's cyberattack industry*, Globes, 25.04.2022, https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066 [access: 23.09.2022].

Bibliography

Azulai Y., *Natanjahu scraps plans to regulate cybersecurity*, Globes, 19.04.2016, https://en.globes.co.il/en/article-netanyahu-scraps-plans-to-regulate-cyber-security-cos-1001118937 [access: 21.09.2022].

Cornish P., *The Oxford Handbook of Cyber Security*, Oxford 2021.

Eichensehr K.E., *Public-private cybersecurity*, „Texas Law Review" 2017, vol. 95.

Forrester Ch., *Israel tightens regulations around cyber exports*, Janes.com, 7.12.2021, https://www.janes.com/defence-news/news-detail/israel-tightens-regulations-around-cyber-exports [access: 22.09.2022].

France and Israel hold 'secret' talks to defuse phone spyware row, The Guardian, 22.10.2021, https://www.theguardian.com/world/2021/oct/22/france-and-israel-hold-secret-talks-to-defuse-phone-spyware-row [access: 23.09.2022].

Gilead A., *Export controls strangling Israel's cyberattack industry*, Globes, 25.04.2022, https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066 [access: 23.09.2022].

Hindin D., *Can Export Controls Tame Cyber Technology?: An Israeli Approach*, Lawfare, 12.02.2016, https://www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach [access: 21.09.2022].

Huang K., *Chief of Israeli Spyware Firm NSO to Step Down as It Revamps*, New York Times, 21.08.2021, https://www.nytimes.com/2022/08/21/business/nso-chief-executive-spyware.html [access: 22.09.2022].

Iliescu A., *Israeli import, export, cyber regulation & enforcement*, Shibolet law, 19.05.2020, https://www.shibolet.com/en/israeli-import-export-and-cyber-regulation-and-enforcement/ [access: 21.09.2022].

Margolis N., *Work in progress? Israeli export control regulators face up to new challenges*, „WorldECR" 2021, issue 102.

Pyetranker I., An Umbrella in a Hurricane: Cyber Technology and the December 2013 Amendment to the Wassenaar Arrangement, „Northwestern Journal of Technology and Intellectual Property" 2015, vol. 13/2, no. 3.

Schmitt M., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge 2017.

Shulman S., *As cyber wars escalates Israeli tech gains an edge'*, CTech, 2.04.2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3902572,00.html [access: 21.09.2022].

Tabansky L., Ben Israel I., *Cybersecurity in Israel*, New York 2015.

The future of discussions on ICTs and cyberspace at the UN, 10.08.2020, https://tiny.pl/95bk8 [access: 20.09.2022].

Transparency and Accountability Report 2021, https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf [access: 22.09.2022].

Vadakkanmarveettil J., *Why the Israelis lead the world in cyber security expertise*, Jigsawacademy, 27.01.2020, https://www.jigsawacademy.com/why-the-israelis-lead-the-world-in-cyber-security-expertise/ [access: 21.09.2022].

Czy można było zapobiec Pegasus Gate? Ewolucja systemu kontroli eksportu narzędzi do cyberinwigilacji w Izraelu

Streszczenie

Przedmiotem niniejszego artykułu jest omówienie przepisów prawnych regulujących w izraelskim i międzynarodowym systemie prawnym kontrolę obrotu narzędziami służącymi do cyberinwigilacji. Przeprowadzona została szczegółowa analiza obowiązujących regulacji, której celem jest klasyfikacja i wskazanie niedoskonałości w treści obowiązujących przepisów. Autor identyfikuje zmiany w treści porozumienia z Wassenaar, które spowodowały, że w 2016 roku podjęto próbę bardziej kompleksowego uregulowania kontroli obrotu narzędziami do cyberinwigilacji w prawie izraelskim. Na przykładzie skutków międzynarodowej afery z oprogramowaniem NSO autor pokazuje rolę skutecznego reżimu kontroli eksportu, w tym regulacji międzynarodowych, w zapobieganiu wykorzystywania narzędzi służących do cyberinwigilacji w sposób niebezpieczny dla wartości uznawanych na arenie międzynarodowej.

Słowa kluczowe: cybernadzór, kontrola eksportu, porozumienie z Wassenaar, cyberobrona

Monika Nowikowska*

Procesowa kontrola danych informatycznych w chmurze obliczeniowej

Streszczenie

Autorka artykułu podjęła próbę analizy procesowej kontroli korespondencji przechowywanej w pamięci wirtualnej, czyli w tzw. chmurze (cloud computing). Opracowanie stanowi próbę odpowiedzi na pytanie, w jaki sposób urządzenia mobilne i chmury są badane i jaki wpływ na realizację czynności procesowych mają przepisy prawa odnośnie do prywatności. Wzrost zainteresowania chmurą obliczeniową skutkuje pojawieniem się wielu nowych problemów prawnych, które przekładają się m.in. na praktykę i zasady działania organów ścigania. W pierwszej kolejności omówiono pojęcie „chmura obliczeniowa" oraz poddano analizie przepisy dotyczące pozyskiwania dowodów elektronicznych. Uniezależnienie systemów teleinformatycznych od funkcjonowania klasycznego środowiska pracy opartego na pojedynczej stacji roboczej pozwoliło także postawić pytanie o transgraniczność usług świadczonych w chmurze. Dane informatyczne przekazywane poprzez chmurę obliczeniową mogą być zapisywane na kilkunastu urządzeniach zlokalizowanych w różnych państwach.

Słowa kluczowe: chmura obliczeniowa, obrazowanie fizyczne, obrazowania logiczne, przeszukanie, zabezpieczenie dowodów

* Dr Monika Nowikowska, adiunkt w Katedrze Prawa Informatycznego, Wydział Prawa i Administracji, Akademia Sztuki Wojennej, radca prawny, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

Wstęp

Rozwój nowych technologii daje z jednej strony możliwości samorealizacji jednostki, z drugiej, niesie za sobą zagrożenia. Wraz ze wzrostem możliwości i złożoności urządzeń mobilnych wzrosła zarówno liczba ich użytkowników, jak i ilość informacji przechowywanych na tych urządzeniach. Przykładowo, najnowsze smartfony mają możliwość obsługi kart pamięci o pojemności 1 Tb[1]. Prowadzi to do sytuacji, w której użytkownicy przechowują w swoich smartfonach ogrom danych i informacji, w tym dane wrażliwe ze sfery życia prywatnego[2].

Łatwość dostępu do nowych technologii oraz ich powszechność sprawia, że ten obszar działalności człowieka staje się także narzędziem działań przestępczych[3]. Nie jest zaskoczeniem, że wraz ze wzrostem liczby urządzeń rośnie potencjał przechowywania przez nie istotnych danych dla procesu karnego. To wszystko czyni ze smartfonów, komputerów i internetu także narzędzie do popełniania przestępstw[4].

W artykule podjęto próbę analizy operacyjnej i procesowej kontroli korespondencji przechowywanej w pamięci wirtualnej, czyli w tzw. chmurze (cloud computing – CC)[5]. Na wstępie należy zauważyć, że jest to temat ważny i złożony, gdyż dochodzi w tym przypadku do kolizji dwóch dóbr – naturalnej antynomii pomiędzy bezpieczeństwem państwa (czynności operacyjne i procesowe) a prywatnością jednostki[6]. Czynność procesowa polegająca na przeszukaniu mieszkania lub osoby stanowi wyjątek od konstytucyjnie zagwarantowanej nienaruszalności mieszkania i korespondencji (art. 49 i 50 Konstytucji RP[7]) i musi być stosowana z bardzo dużą rozwagą. Z drugiej strony, zwiększona

1 https://www.apple.com/pl/iphone-13-pro/specs/ [dostęp: 2.09.2022].

2 K. Chałubińska-Jentkiewicz, M. Nowikowska, *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020, s. 216; A. Etzioni, *Privacy in a cyber age, Policy and Practice*, Hampshire 2015, s. 67.

3 A. Gobeo, C. Fowler, W.J. Buchanan, *GDPR and Cyber Security for Business Information Systems*, Gistrup 2018, s. 99.

4 M. Siwiecki, P. Kowalski, *Przeszukanie i zatrzymanie rzeczy w sprawach o cyberprzestępstwa. Udział specjalistów i biegłych w czynnościach procesowych*, „Kwartalnik Policyjny" 2021, t. 57, nr 2, s. 3.

5 E. Molenda-Kropielnicka, *Cloud Computing – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2013, nr 119, s. 113.

6 D. Szumiło-Kulczycka, *Między ochroną prywatności a bezpieczeństwem – uwagi na tle orzecznictwa ETPCz i TSUE* [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017, s. 68.

7 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483.

świadomość zarówno obywateli, jak i producentów urządzeń ochrony danych doprowadziła do tego, że urządzenia te są bardziej bezpieczne, ale odbywa się to kosztem bezpieczeństwa i zdolności organów ścigania do zwalczania nielegalnych działań[8]. Należy zauważyć, że w sprawach karnych sukces dochodzenia może zależeć od zdolności śledczego do uzyskania dostępu do dowodów przechowywanych zarówno w urządzeniu mobilnym, jak i w chmurze. Artykuł stanowi próbę odpowiedzi na pytanie: w jaki sposób urządzenia mobilne i chmury są badane i jaki wpływ na realizację czynności procesowych mają przepisy prawa odnośnie do prywatności. W pierwszej kolejności omówienia wymaga pojęcie „chmura obliczeniowa". W dalszej kolejności analizie poddano przepisy dotyczące pozyskiwania dowodów elektronicznych. Wzrost zainteresowania chmurą obliczeniową skutkuje pojawieniem się wielu nowych problemów prawnych, które przekładają się m.in. na praktykę i zasady działania organów ścigania. Podczas wykonywania czynności operacyjno-rozpoznawczych czy dochodzeniowo-śledczych pojawia się konieczność uwzględnienia transgraniczności, dlatego że dane informatyczne przekazywane poprzez chmurę obliczeniową mogą być zapisywane na kilkunastu urządzeniach zlokalizowanych w różnych państwach[9]. Uniezależnienie systemów teleinformatycznych od funkcjonowania klasycznego środowiska pracy opartego na pojedynczej stacji roboczej nasuwa także pytanie o potrzebę reinterpretacji tradycyjnego rozumienia miejsca popełnienia przestępstwa oraz zabezpieczenia mienia w celach dowodowych, które wiąże się zarówno z przeszukaniem, jak i zabezpieczeniem danych przechowywanych na nośnikach zlokalizowanych w jednym państwie[10].

Cloud computing – ogólna charakterystyka (pojęcie, cechy, funkcje)

Chmura obliczeniowa jest modelem gwarantującym wszechobecny, wygodny, szybki i możliwy na żądanie dostęp do dzielonych zasobów obliczeniowych (serwerów, pamięci masowej, aplikacji, usług) za pośrednictwem sieci.

8 D. Kahvedžic, *Digital forensics and DSAR effect in ERA Forum*, t. 22, Berlin 2021, s. 356.
9 F. Casino i in., *SoK: cross-border criminal investigations and digital evidence*, „Journal of Cybersecurity" 2022, t. 8, s. 1–18.
10 M. Siwicki, *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2015, nr 1–2, s. 31.

W literaturze przedmiotu podkreśla się, że zasoby te są zapewniane i uwalniane przy minimalnym zarządzeniu i ingerencji dostawcy[11]. Telefon czy komputer przestają być nośnikiem danych. Dane są przenoszone do wirtualnych pamięci zewnętrznych. Ułatwienia kierowane do użytkowników związane z funkcjonowaniem chmury, przy braku szczegółowej regulacji w tym zakresie, stają się także nowym wyzwaniem dla organów porządku publicznego[12].

Należy podkreślić, że usługa przetwarzana w chmurze wykazuje podobieństwo do outsourcingu. Polega ona na wykorzystywaniu cudzych programów komputerowych, infrastruktury, narzędzi programistycznych hostowanych przez dostawcę w celu tworzenia własnych aplikacji.

W przypadku tych nowych metod przetwarzania danych prawie wszystkie zadania obliczeniowe, w tym: instalacja, administrowanie usługami i przesyłanie danych, odbywają się niezależnie od lokalizacji poszczególnych elementów fizycznych sprzętu komputerowego. Cechą użytkowania CC jest uniezależnienie systemów teleinformatycznych od użytkowanego sprzętu. Trafnie zauważa Maciej Siwicki, że „[...] szczególną cechą wskazanych usług jest zatem tzw. wirtualizacja, a więc oddzielenie warstwy logicznej od warstwy fizycznej systemu informatycznego, dzięki połączeniu wirtualnych maszyn w jeden fizyczny serwer oraz uniezależnieniu funkcjonowania systemu IT użytkownika od funkcjonowania klasycznego środowiska pracy, opartego zazwyczaj na pojedynczej stacji roboczej i jednym systemie operacyjnym”[13]. Kolejną cechą, na którą zwraca on uwagę, jest to, że dane informatyczne, np. pliki zawierające dokumenty tekstowe, w trakcie przesyłania do użytkownika mogą być w tym czasie zapisywane w kilku miejscach, tzn. na serwerach, które mogą być zlokalizowane w różnych państwach. Wskazuje to, że chmura bazuje na współdziałaniu, udostępnianiu i możliwości korzystania z zasobów informacyjnych niezależnie od geograficznej lokalizacji poszczególnych jej elementów[14]. Należy zauważyć, że rozproszenie zasobów informatycznych jest dokonywane głównie ze względów funkcjonalnych i związane z charakterystyką techniczną chmury obliczeniowej, która polega na wyszukiwaniu najkorzystniejszego miejsca zapisu. Miejscem stałego zapisu danych nie będzie komputer,

11 J. Wrona, Z. Zawadzka, *Cyberbezpieczeństwo w prawie własności intelektualnej* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018, s. 377–378.

12 J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo” 2017, nr 8–7, s. 31.

13 M. Siwicki, op. cit., s. 32–33.

14 J. Kudła, A. Staszak, op. cit., s. 32.

z którego korzysta użytkownik. Oznacza to, że użytkownik nie jest zarówno właścicielem sprzętu, na którym są zapisywane jego dane, jak i nie zna lokalizacji[15]. Ta cecha funkcjonowania CC implikuje poważne problemy prawne z punktów widzenia funkcjonowania organów ścigania. Z powodu konieczności określenia lokalnego miejsca zapisu danych utrudnione jest określenie właściwości miejscowej sądu czy też uprawnień poszczególnych organów ścigania.

Zagadnienie CC zostało poruszone w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS)[16]. W preambule w pkt 17 wskazano, że usługi przetwarzania w chmurze obejmują szeroki zakres działań, które mogą być realizowane według różnych modeli. Ustawodawca unijny pojęciem „usługi przetwarzania w chmurze" objął usługi, które umożliwiają dostęp do skalowalnego i elastycznego zbioru zasobów komputerowych do wspólnego wykorzystywania. Tak skonstruowane pojęcie pozwala na wyróżnienie czterech elementów: 1) skalowanie, 2) elastyczny zbiór, 3) zasoby obliczeniowe, 4) wspólne wykorzystywanie.

Skalowalnie odnosi się do zasobów komputerowych, które są elastycznie przydzielane przez dostawcę usługi niezależnie od położenia geograficznego zasobów jako reakcja na zmiany zapotrzebowania.

Pojęcie „elastyczny zbiór" odnosi się do opisu tych zasobów obliczeniowych, które są przydzielane i uwalniane zależnie od zapotrzebowania, żeby szybko zwiększać i zmniejszać dostępne zasoby w zależności od obciążenia.

Przez zasoby obliczeniowe rozumie się takie zasoby, jak: sieci, serwery lub inną infrastrukturę, pamięć, aplikacje i usługi.

Pojęcie „wspólne wykorzystywanie" dotyczy opisu zasobów obliczeniowych udostępnianych wielu użytkownikom, którzy dzielą wspólny dostęp do usługi, ale przetwarzanie odbywa się oddzielnie dla każdego z nich, mimo że usługa ta jest świadczona z tego samego sprzętu elektronicznego. Zgodnie z art. 4 pkt 5 dyrektywy NIS usługę przetwarzania w chmurze należy zaliczyć do rodzaju usług cyfrowych[17].

15 M. Siwicki, op. cit., s. 33.

16 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. Urz. UE 2016, L 194/1.

17 K. Chałubińska-Jentkiewicz, *Prawna ochrona treści cyfrowych*, Warszawa 2022, s. 66 i n.

Pojęcie chmury obliczeniowej zostało także opisane w komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Wykorzystanie potencjału chmury obliczeniowej w Europie"[18]. Model chmury obliczeniowej zdefiniowano w nim jako przechowywanie, przetwarzanie i wykorzystanie danych, do których dostęp uzyskuje się przez internet, na znajdujących się w innej lokalizacji komputerach. Oznacza to, że użytkownicy mogą na życzenie dysponować nieograniczonymi mocami obliczeniowymi, nie muszą dokonywać znacznych inwestycji kapitałowych w celu zrealizowania swoich potrzeb oraz mogą uzyskiwać dostęp do swoich danych z każdego miejsca, w którym mają połączenie z internetem. W komunikacie wskazano ponadto, że dzięki chmurze obliczeniowej będzie możliwe ograniczenie wydatków użytkowników na technologie informacyjne (IT) oraz opracowanie nowych usług. O ile światowa sieć internetowa (World Wide Web) oferuje dostęp do informacji wszystkim i wszędzie, o tyle chmura obliczeniowa pozwala na dostęp wszystkim i wszędzie do mocy obliczeniowej.

Reasumując, chmurę obliczeniową można określić jako model informatyzacji, w którym do realizacji zadań informatycznych, czyli przechowywania i przetwarzania danych, wykorzystuje się zewnętrzne, tj. znajdujące się poza przedsiębiorstwem, zasoby komputerowe (sprzęt, oprogramowanie) udostępniane użytkownikom z wykorzystaniem internetu[19].

Chmura obliczeniowa bazuje na architekturze zorientowanej na usługi informatyczne (Service-Oriented Architecture). Główną funkcją chmury obliczeniowej jest dostarczanie na życzenie użytkownika różnego rodzaju usług. Do tych najpopularniejszych należą: 1) chmura aplikacyjna (cloud applications) – obejmuje ona usługi związane z dostarczaniem i dystrybucją oprogramowania. Software as a Service (SaaS) – oprogramowanie jako usługa, w tym model sprzętu, platforma oraz odpowiednio skonfigurowane aplikacje udostępniane są przez usługodawcę użytkownikowi[20]. Użytkownik końcowy widzi w swoim systemie tylko i wyłącznie aplikacje, z których korzysta. Sprzęt i platforma nie są dla użytkownika widoczne – działają one na serwerze dostawcy (usługodawcy), dostęp do nich ma tylko usługodawca. Jednym z elementów

18 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Wykorzystanie potencjału chmury obliczeniowej w Europie, COM/2012/0529 final.

19 J. Kudła, A. Staszak, op. cit., s. 39; J. Jurek, *Wdrożenia informatycznych systemów zarządzania*, Warszawa 2016, s. 70–73.

20 Ł. Pirożek, *Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6, s. 76.

dotyczącym udostępniania oprogramowania w modelu SaaS jest interfejs użytkownika; 2) chmura ze „środowiskiem oprogramowania" (Cloud Software Environment) określana jest także jako PaaS – Platform as a Service. Polega ona na udostępnianiu przez dostawcę wirtualnego środowiska (platformy) pracy. W tym modelu użytkownik otrzymuje komplet aplikacji, co nie wiąże się z koniecznością zakupu przez użytkownika sprzętu ani instalacją oprogramowania. Użytkownik ma dostęp do interfejsu poprzez program klienta – przeglądarkę internetową. Świadczone usługi są dostępne z dowolnego komputera połączonego z siecią internet; 3) chmura z infrastrukturą do oprogramowania (Cloud Software Infrastructure) obejmuje infrastrukturę informatyczną, czyli sprzęt, serwery odpowiedzialne za uruchamianie istniejących aplikacji i systemów operacyjnych (Infrastructure as a Service – IaaS), usługi związane z przechowywaniem i gromadzeniem danych oraz udostępnianie ich na żądanie użytkownika (Data as a Service – DaaS) oraz usługi związane z zapewnieniem optymalizacji pracy programów poprzez kontrolę ich środowiska działania i procesu translacji kodu (Communications as a Service – CaaS). Infrastruktura jako usługa IaaS to model, w którym usługodawca dostarcza usługobiorcy cały sprzęt, infrastrukturę informatyczną, czyli oprogramowanie, usługi serwisowania, komputery, urządzenia do przechowywania danych, serwery. Co do zasady sprzęt ten jest własnością dostawcy usług w chmurze obliczeniowej, a nie użytkownika, który uzyskuje jedynie dostęp do chmury za pośrednictwem internetu[21]. Komunikacja jako usługa (Communications as a service – Caas) polega na tym, że usługodawca zapewnia platformę pod telekomunikacyjne środowisko pracy.

Inny prezentowany podział chmury obliczeniowej wyróżnia chmury prywatną, publiczną i hybrydową. Wszystkie zasoby chmury prywatnej są przeznaczone do korzystania tylko dla jednego podmiotu. Chmura prywatna może być usługą albo infrastrukturą przeznaczoną dla jednego klienta i nie jest dostępna dla innego użytkownika. Zasoby chmury publicznej udostępnia się wielu odbiorcom, którzy mogą korzystać z tego samego sprzętu i oprogramowania. Różnica polega na tym, że w przypadku chmury publicznej dostawca powinien zapewnić odpowiednią separowalność danych[22]. W przypadku chmury hybrydowej część jej zasobów jest przeznaczona do korzystania dla jednego wyznaczonego podmiotu, inna zaś jej część jest udostępniana publicznie.

21 M. Siwicki, op. cit., s. 31; J. Kudła, A. Staszak, op. cit., s. 39.
22 Ibidem, s. 41.

Podsumowując przeprowadzone rozważania, można stwierdzić, że chmura obliczeniowa nie jest ograniczona geograficznie i co do zasady dostępna jest z każdego miejsca na świecie. Tworzy ona zbiór usług cyfrowych, i jest stale rozwijana. Wykorzystany sprzęt w chmurze obliczeniowej co do zasady nie jest dostępny dla użytkownika końcowego i często nie ma on wiedzy, który sprzęt i w jakim momencie faktycznie go obsługuje. W celu możliwie najlepszego wykorzystania sprzętu w chmurze obliczeniowej dostawcy usług często przenoszą dane i aplikacje poszczególnych użytkowników.

Można wskazać następujące cechy chmury obliczeniowej: 1) samoobsługa na żądanie – dostęp do nowych zasobów obliczeniowych jest możliwy bez konieczności kontaktu z dostawcą usługi; 2) nieograniczony dostęp do sieci za pośrednictwem każdego urządzenia z dostępem do internetu; 3) wielodzierżawa, tj. agregacja pozwalająca na gromadzenie i dzielenie zasobów między wielu użytkowników jednocześnie; 4) elastyczność; 5) mierzalność usługi (zakres i intensywność korzystania z danej usługi musi być na bieżąco monitorowania)[23].

Użytkownicy mogą korzystać z usługi przetwarzania w chmurze obliczeniowej w celu przechowywania na tzw. serwerze wirtualnym wszystkich dostępnych informacji. Dane te, w postaci różnego rodzaju dokumentów cyfrowych, są przekazywane do zasobów chmury obliczeniowej np. pocztą elektroniczną. Tak zapisane w chmurze pliki cyfrowe pozwalają na ich odtworzenie w momencie dowolnie wybranym przez użytkownika.

Podstawy prawne dostępu organów procesowych do danych przechowywanych w chmurze obliczeniowej

W prawie polskim zagadnienie przeszukania środowiska informatycznego zostało uregulowane w ustawie z 6 czerwca 1997 roku kodeks postępowania karnego[24]. Regulacje dotyczące pozyskiwania dowodów elektronicznych[25] znajdują się przede wszystkim w art. 217, 218, 218a, 219, 236a, 237, 241.

23 E. Molenda-Kropielnicka, op. cit., s. 111; J. Wrona, Z. Zawadzka, op. cit., s. 378; F. Radoniewicz, *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, nr 2, s. 152–153.

24 Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, t.j., Dz.U. 2022, poz. 1375, z późn. zm.

25 A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 94.

Procesowe zasady przeszukania i zatrzymania danych informatycznych

Na wstępie należy zaznaczyć, że rozdział 25 k.p.k. jest poświęcony zatrzymaniu rzeczy i przeszukaniu. Podstawą przeszukania jest uzasadnione podejrzenie, że osoby poszukiwane lub poszukiwane rzeczy (dane informatyczne) znajdują się tam, gdzie są poszukiwane[26]. Należy podkreślić, że danych informatycznych nie należy traktować jako rzeczy w rozumieniu karnoprocesowym. Dane informatyczne stanowią odrębną kategorię niematerialnych źródeł dowodowych[27]. Przepisy rozdziału 25 „Zatrzymanie rzeczy. Przeszukanie", zgodnie z art. 236a k.p.k., znajdują do nich jednak odpowiednie zastosowanie. Dyspozycja art. 236a stanowi, że „[...] przepisy rozdziału niniejszego stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną".

Należy wyraźnie wskazać różnice i oddzielić przeszukanie od zatrzymania rzeczy, które zostały określone w art. 217 i 219 k.p.k. Od zatrzymania rzeczy przeszukanie różni się przede wszystkim wyższym stopniem ingerencji, gdyż łączy się z penetracją pomieszczeń, odzieży, zasobów pamięci systemu informatycznego. Ponadto przeszukanie stanowi wykrywczą czynność dowodową, która jednocześnie jest środkiem przymusu pozwalającym na wkroczenie w określoną sferę praw i wolności jednostki[28].

W wypadku pozyskiwania danych przetwarzanych w chmurze zastosowanie znajdzie art. 217 k.p.k. w zw. z art. 236a, zgodnie z którym możliwe jest żądanie wydania danych przechowywanych na urządzeniu, w systemie lub na nośniku od dysponenta lub użytkownika tego urządzenia, nośnika lub systemu. Po drugie, możliwe będzie także przeszukanie urządzenia lub systemu informatycznego w celu znalezienia danych mogących stanowić dowód w sprawie na podstawie art. 219 w zw. z art. 236a k.p.k. Wreszcie, możliwe jest żądanie wydania korespondencji elektronicznej oraz wykazów połączeń teleinformatycznych na podstawie art. 218 w zw. z art. 236a k.p.k.

Należy podkreślić, że nie chodzi tu o przeszukanie w znaczeniu tradycyjnym, ale o penetrację[29] – przy użyciu odpowiedniego oprogramowania –

26 M. Siwiecki, P. Kowalski, op. cit., s. 4.
27 M. Siwicki, op. cit., s. 37; A. Lach, op. cit., s. 94.
28 M. Siwiecki, P. Kowalski, op. cit., s. 4.
29 M. Siwicki, op. cit., s. 37.

zawartych w urządzeniu lub systemie danych w celu znalezienia i zabezpieczenia ich dla procesu. Istotne jest tu rozróżnienie danych technicznych – związanych z przekazem informacji, miejsca logowań do systemu, wielkości i charakterystyki przekazywanych plików – od danych merytorycznych, treściowo istotnych z punktu widzenia realizacji celów postępowania karnego.

Dane te na urządzeniu mobilnym mogą znajdować się w pamięci urządzenia lub systemie plików. System plików jest organizowany i zarządzany przez system operacyjny urządzenia (SO)[30]. W przypadku utworzenia przez użytkownika informacji system operacyjny określa, gdzie w systemie plików można zapisać dane i zarządza sposobem ich pobierania. W przypadku usunięcia danych SO usuwa te informacje z systemu plików. Zdarza się, że system operacyjny nie usuwa informacji z systemu plików, usuwa jedynie odniesienie do tej części systemu. W takim wypadku dane pozostają w systemie plików do momentu, w którym zostaną nadpisane nowymi danymi. Dane te można także odzyskać za pomocą odpowiedniego oprogramowania[31].

Stosowane oprogramowanie kryminalistyczne powinno wydobywać zarówno dane znajdujące się na urządzeniu, jak i wszelkie usunięte informacje. Zasadne jest opracowywanie takich oprogramowań dla organów procesowych, które zapewniałyby, że wszystkie dane odzyskane z urządzeń są wiarygodne, dokładne i mogą być wykorzystane jako dowody w postępowaniu sądowym. Oprócz zapewnienia, że odpowiednie dane (merytoryczne treściowo z punktu widzenia realizacji celów postępowania karnego) zostaną pobrane ważne jest także zapewnienie, że proces ten jest przejrzysty i możliwy do zweryfikowania. Szczególnie ważne jest upewnienie się, że dane na urządzeniu nie zostały w żaden sposób zmodyfikowane. Dostęp do kryminalistycznych urządzeń zbierających dane powinien być kontrolowany, a wszystkie dane przeniesione do kopii zapasowej. Oznacza to, że wszelkie analizy powinny być wykonywane na skopiowanych danych, podczas gdy oryginał jest bezpiecznie przechowywany[32].

Procesowe zasady kontroli i utrwalania rozmów

Rozdział 26 k.p.k. jest poświęcony kontroli i utrwalaniu rozmów. Po wszczęciu postępowania sąd, na wniosek prokuratora, może zarządzić kontrolę i utrwalanie treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla

30 W iPhonach system ten nosi nazwę iOS lub Android w smartfonach Google.
31 D. Kahvedžic, op. cit., s. 358.
32 Ibidem, s. 360.

toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Ustawodawca w art. 237 § 3 k.p.k. w katalogu zamkniętym wskazał enumeratywnie przestępstwa, co do których można przeprowadzać tę czynność. W literaturze przedmiotu słusznie podkreśla się, że zarządzenia podsłuchu telefonicznego w sprawie o przestępstwo niekatalogowe nie uzasadnia nawet interes społeczny wielkiej wagi[33].

Zgodnie z art. 241 k.p.k. przepisy rozdziału o kontroli i utrwalaniu rozmów stosuje się odpowiednio do kontroli oraz do utrwalania z wykorzystaniem środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Oznacza to, że dopuszczalne jest podsłuchiwanie treści wiadomości przesyłanych przez internet. Jednakże warto zauważyć, że ustawa ogranicza pod względem przedmiotowym stosowanie podsłuchu do enumeratywnie wyliczonych w § 3 art. 237 k.p.k. najcięższych przestępstw. Zdaniem Siwickiego „[...] takie przedmiotowe ograniczenie podsłuchu komputerowego powoduje sytuację, w której jego zastosowanie będzie wyłączone w stosunku do najczęstszych cyberprzestępstw. Obecnie zakresem zastosowania kontroli i utrwalania treści rozmów objęte będą mogły być jedynie sprawy o szpiegostwo lub ujawnienie informacji niejawnych o klauzuli tajności »tajne« lub »ściśle tajne«, przechowywanych w chmurze obliczeniowej”[34]. Jedną z technik pozwalających analizować pakiety przesyłane przez sieć komputerową jest tzw. głęboka inspekcja pakietów (Deep Packet Inspection).

Transgraniczność usług świadczonych w chmurze

Dane przechowywane w chmurze mogą stanowić ważny dowód w postępowaniu sądowym. Obecne narzędzia kryminalistyczne mają możliwości wyodrębnienia potencjalnych dowodów z chmury z urządzenia mobilnego. Wprawdzie nie mogą one otrzymać dostępu do samej usługi w chmurze, ale dostarczają wskazówek, do których usług w chmurze mógł być uzyskany dostęp[35].

Można ponadto wywnioskować, które chmury prawdopodobnie zostały użyte na podstawie typu danego urządzenia. Apple iPhone posiada głęboką

33 K. Boratyńska, P. Czarnecki, A. Lach, *Komentarz do art. 237 k.p.k.* [w:] *Kodeks postępowania karnego*, *Komentarz*, red. A. Sakowicz, Warszawa 2023.
34 M. Siwicki, op. cit., s. 37.
35 D. Kahvedžic, op. cit., s. 364.

integrację z iCloud, telefony z systemem Android korzystają z Google Drive, a telefony z systemem Windows zazwyczaj z OneDrive firmy Microsoft. W najnowszych urządzeniach korzystanie z chmury jest wyraźnie zachęcane już przy pierwszym uruchomieniu urządzenia. Przyjęcie chmury jako zewnętrznego medium pamięci masowej wzrosło ze względu na darmową (lub tanią) jej dostępność oraz rosnącą szybkość łączności, na którą pozwalają szybsze sieci telekomunikacyjne. Jako przykład można wskazać aplikację Microsoft Office, która pozwala użytkownikom zapisywać swoje dokumenty poza urządzeniem bezpośrednio do chmury Microsoftu. Jest to jeden z przykładów oprogramowania łączącego swoje usługi z chmurą. Dostęp do chmury jest coraz częściej ułatwiony i zintegrowany z istotą funkcjonalności urządzenia.

Przeszukanie danych w chmurze stawia przed organami ścigania nowe wyzwania. Głównym problemem jest to, że dane są przechowywane przez dostawcę chmury w imieniu użytkownika. Użytkownik – co do zasady – nie wie, gdzie dane są przechowywane dopóki może je odzyskać za pomocą urządzenia mobilnego. Wszechobecność danych jest jedną z głównych cech chmury, ale jest również jednym z głównych problemów organów śledczych[36].

Międzynarodowy charakter chmury obliczeniowej może utrudniać prowadzenie śledztwa i pozyskiwanie dowodów elektronicznych. Należy podkreślić, że w przeciwieństwie do urządzenia mobilnego, miejscem przechowywania danych w chmurze jest centrum danych należące do dostawcy chmury, do którego nie można uzyskać dostępu ani go przejąć w taki sam sposób jak do urządzeń mobilnych. Organy procesowe przy użyciu specjalistycznych urządzeń nie mogą uzyskać dostępu do danych bez właściwych danych uwierzytelniających użytkownika.

Dla pozyskiwania dowodów z urządzeń mobilnych podstawowe znaczenie ma obrazowanie. Metoda ta polega na wyodrębnianiu kopii wszystkich informacji przechowywanych w systemie plików urządzenia. Celem tego procesu jest stworzenie dokładnego duplikatu danych, co umożliwia organowi ścigania przeprowadzenie dokładnego dochodzenia na kopii danych urządzenia, a nie na oryginale.

Oprócz wydobywania danych, które były widziane i do których użytkownik ma dostęp, specjalistyczne oprogramowania stosowane przez organy ścigania mają także możliwość zobrazowanie informacji wcześniej usuniętych. Dostęp do tych obszarów jest zwykle uniemożliwiony przez system operacyjny

36 Ibidem, s. 362.

urządzenia. Z punktu widzenia przeszukania i zdobycia istotnych informacji ważne jest obejście tych zabezpieczeń i uzyskanie dostępu do tych obszarów w sposób kontrolowany, żeby ujawnić ukryte w nich informacje.

W literaturze przedmiotu wskazuje się dwa główne rodzaje obrazowania, tj. fizyczne i logiczne[37].

Obrazowanie fizyczne jest metodą, w której system operacyjny urządzenia jest całkowicie pomijany, a wszystkie informacje są odczytywane bezpośrednio z systemu plików. Zapewnia ona, że wszystkie dane, które znajdują się na urządzeniu, są z niego kopiowane. Gwarantuje to, że wszystkie usunięte, ukryte i tymczasowe pliki są niezawodnie kopiowane bez oporu przez jakiekolwiek zabezpieczenia systemu operacyjnego. Poprzez pominięcie systemu operacyjnego uprawniony organ nie wie jak pliki są zorganizowane w systemie plików. Fizyczne wyodrębnianie danych jest wykonywane najrzadziej, ponieważ uzyskanie pełnego dostępu do pamięci wewnętrznej urządzenia mobilnego jest całkowicie zależne od systemu operacyjnego i środków bezpieczeństwa zastosowanych przez producentów. Fizyczne wydobywanie danych z urządzenia mobilnego opiera się na tej samej podstawowej koncepcji, co fizyczne obrazowanie kryminalistyczne dysku twardego komputera (kopia binarna). Fizyczne pozyskiwanie polega na wykonywaniu kopii bit po bicie całej zawartości pamięci flash urządzenia mobilnego. Ta metoda umożliwia gromadzenie wszystkich danych istniejących, a także danych, które zostały usunięte lub są ukryte przez użytkownika[38].

Obrazowanie logiczne to proces, w którym dane są zbierane za pomocą systemu operacyjnego. Oprogramowanie do obrazowania żąda danych od systemu operacyjnego i zbiera dane, które są mu dostarczane. Ten proces obrazowania zależy od dostępu, który umożliwia system operacyjny. W obrazowaniu logicznym narzędzia kryminalistyczne komunikują się z systemem operacyjnym urządzenia mobilnego. Proces pozwala na pobieranie większości widocznych danych. Urządzenie do badania musi zostać uruchomione (następuje nieuniknione, ale udokumentowane naruszenie integralności danych)[39].

Proces obrazowania logicznego pozwala na zebranie takich danych, jak m.in.: dzienniki połączeń, SMS, zdjęcia, nagrania wideo, kontakty. Nie jest on tak kompleksowy jak proces obrazowania fizycznego. Jest to po prostu zbiór

37 Ibidem, s. 360.
38 *Mobilna informatyka śledcza*, https://olszta.it/strona-1/mobilna-informatyka-sledcza/ [dostęp: 2.01.2023].
39 Ibidem.

treści, które OS umożliwia badaczowi. System operacyjny nie pobiera żadnych informacji, do których nie ma dostępu, takich jak wcześniej usunięte pliki. Obrazowanie logiczne przeprowadza się tylko wtedy, kiedy nie ma dostępu do fizycznego systemu plików lub nie jest znany sposób, w jaki system operacyjny przechowuje swoje pliki. Obrazowanie fizyczne jest zawsze preferowaną metodą, ponieważ skutkuje bardziej niezawodnym i kompleksowym przechwytywaniem danych[40].

W tym miejscu należy podkreślić, że dostawcy usług działają w imieniu użytkowników i są zobowiązani do zapewnienia ochrony prywatności i bezpieczeństwa ich danych. Prywatność i bezpieczeństwo danych odgrywają coraz większą rolę w opracowywaniu urządzeń przez producentów[41]. Coraz częściej urządzenia są blokowane za pomocą złożonego kodu, wzoru, hasła lub odcisku palca. Skutkuje to rygorystycznymi kontrolami dostępu, a przede wszystkim domyślnym pełnym szyfrowaniem dysku. Przykładowo, po ustawieniu kodu PIN w telefonie iPhone wszystkie dane na urządzeniu są zaszyfrowane i nie mogą być dostępne dla nieuprawnionych użytkowników. Według szacunków firmy Apple odgadnięcie kodu PIN poprzez wypróbowanie wszystkich możliwych kombinacji zajęłoby nawet pięć i pół roku. Powoduje to, że w obecnych smartfonach organy ścigania nie mają możliwości odblokowania urządzenia bez kodu dostępu. Producenci urządzeń poprzez wprowadzanie coraz to silniejszych zabezpieczeń uniemożliwiają dowolnej aplikacji bezpośredni dostęp do systemu plików nawet po jego odblokowaniu. Wpływa to na funkcjonowanie organów ścigania, w aspekcie poszukiwania przez nich istotnych dowodów. Funkcje te uniemożliwiają oprogramowaniu kryminalistycznemu zignorowanie systemu operacyjnego i uzyskanie dostępu do systemu plików. Jedynym sposobem, w jaki dane mogą być skopiowane z urządzenia, pozostaje obrazowanie logiczne przez system operacyjny. Oznacza to, że preferowane fizyczne obrazowanie urządzeń raczej nie będzie normą w najbliższej przyszłości, a uprawnione organy będą skupione na metodzie obrazowania logicznego.

Podsumowując, w urządzeniach mobilnych coraz częściej stosuje się szyfrowanie w celu zakodowania danych na urządzeniach w bezpieczny sposób. W połączeniu z silnymi kodami dostęp do urządzenia stał się znacznie trudniejszy dla organów ścigania. Ponieważ producenci zaczęli ograniczać urządzenia poprzez ich zabezpieczenia, otworzyli je zatem także pod względem ich

40 D. Kahvedžic, op. cit., s. 362.
41 Ibidem, s. 364.

integracji z internetem. Dodawane są funkcje, które w coraz większym stopniu opierają się na łatwości i wszechobecności chmury w celu tworzenia kopii zapasowych danych i łączenia użytkownika z różnymi usługami w chmurze. Chmura pozwoliła producentom zaoferować swoim użytkownikom praktycznie nieograniczoną przestrzeń dyskową do celów takich, jak: kopia zapasowa danych osobowych, przepływ danych między urządzeniami czy udostępnianie informacji w sieciach społecznościowych.

W odniesieniu do wydobywania danych z chmury kopię tych danych można uzyskać w taki sam sposób, w jaki na urządzeniu mobilnym dokonuje się przejęć logicznych. Dane są kopiowane z chmury na bezpieczne i kontrolowane urządzenie. Możliwe jest zażądanie kopii danych od dostawcy usług za pomocą odpowiedniego wniosku, wezwania lub nakazu sądowego, ale to dostawca chmury odpowiada na te wnioski i wydobywa te dane. Praktyka w tym zakresie jest niejasna i w dużej mierze zależy od dostawcy. Kolejnym problemem jest to, że dostawcy usług w chmurze tworzą kopie zapasowe danych w wielu lokalizacjach ze względu na redundancję, opóźnienia i tworzenie kopii zapasowych. Dlatego dane mogą znajdować się w wielu jurysdykcjach i mogą podlegać polityce ochrony danych wielu krajów. Jako przykład skutków prawnych można wskazać sprawę Microsoftu. Firma Microsoft odmówiła przekazana danych poczty elektronicznej przechowywanych w Irlandii na wniosek amerykańskich organów ścigania. Microsoft zakwestionował zdolność Stanów Zjednoczonych Ameryki do gromadzenia tych danych za pomocą amerykańskiego nakazu i zwrócił się do amerykańskich organów ścigania, żeby zamiast tego wystąpiły do sądu irlandzkiego o nakaz sądowy[42].

Zakończenie

Chmura obliczeniowa i urządzenia mobilne są ze sobą ściśle powiązane. Oba urządzenia sprawiły, że przechowywanie, tworzenie i udostępnianie danych stało się niezwykle łatwe w codziennym użytkowaniu. Wraz ze wzrostem ilości danych przechowywanych przez te urządzenia wzrosło także zainteresowanie organów ścigania pozyskiwaniem oraz analizą tych informacji.

Do wydobywania danych z urządzeń mobilnych stosowany jest proces zarówno logiczny, jak i fizyczny. Jak wykazano w opracowaniu, obrazowanie

42 Ibidem.

fizyczne jest preferowaną metodą, ponieważ wydobywa wszystkie możliwe przechowywane na urządzeniu dane. Ponieważ producenci urządzeń, w wyniku stosowanych zabezpieczeń, uniemożliwiają innym aplikacjom bezpośredni dostęp do systemu plików, więc uprawnione organy mają utrudniony dostęp do tych danych. Jedynym sposobem skopiowania danych z urządzenia pozostaje obrazowanie logiczne przez system operacyjny. Oznacza to, że preferowane fizyczne obrazowanie urządzeń raczej nie będzie normą w najbliższej przyszłości, a uprawnione organy będą skupione na metodzie obrazowania logicznego.

Przeprowadzone rozważania pozwalają ponadto wskazać na dychotomiczną rolę dostawców usług w chmurze. Z jednej strony odgrywają oni istotną rolę w poszukiwaniu przez uprawnione organy istotnych dowodów, z drugiej, działają oni również w imieniu użytkowników i są zobowiązani do zapewnienia ochrony prywatności i bezpieczeństwa danych swoich użytkowników. Prywatność i bezpieczeństwo danych odgrywają coraz większą rolę w opracowywaniu urządzeń przez producentów. Te same zasady są stosowane przez twórców chmur, co może powodować, że uprawnione organy będą miały coraz trudniejszy lub niemożliwy dostęp do potrzebnych im danych[43].

Wzrost zainteresowania nowym modelem przetwarzania danych – chmurą obliczeniową – wymaga także powszechnej dyskusji na temat potrzeby podjęcia międzynarodowej współpracy w zdobywaniu dowodów cyfrowych. Dane w chmurze charakteryzuje to, że poprzez stosowaną metodę zapisywania informacji na kilkunastu urządzeniach zlokalizowanych w różnych państwach znajdują się one w wielu jurysdykcjach i mogą podlegać polityce ochrony danych wielu krajów.

Bibliografia

Boratyńska K., Czarnecki P., Lach A., *Komentarz do art. 237 k.p.k.* [w:] *Kodeks postępowania karnego, Komentarz*, red. A. Sakowicz, Warszawa 2023.

Casino F. i in., *SoK: cross-border criminal investigations and digital evidence*, „Journal of Cybersecurity" 2022, t. 8.

Chałubińska-Jentkiewicz K., *Prawna ochrona treści cyfrowych*, Warszawa 2022.

Chałubińska-Jentkiewicz K., Nowikowska M., *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne*, Warszawa 2020.

Etzioni A., *Privacy in a cyber age, Policy and Practice*, Hampshire 2015.

Gobeo A., Fowler C., Buchanan W.J., *GDPR and Cyber Security for Business Information Systems*, Gistrup 2018.

Jurek J., *Wdrożenia informatycznych systemów zarządzania*, Warszawa 2016.

43 Ibidem, s. 365.

Kahvedžic D., *Digital forensics and DSAR effect in ERA Forum*, t. 22, Berlin 2021.
Kudła J., Staszak A., *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 8–7.
Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
Molenda-Kropielnicka E., *Cloud Computing – zagadnienia prawne*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2013, nr 119.
Pirożek Ł., *Prawne aspekty świadczenia usług w modelu SaaS przez przedsiębiorcę telekomunikacyjnego*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2015, nr 6.
Radoniewicz F., *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law" 2022, nr 2.
Siwicki M., *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, „Palestra" 2015, nr 1–2.
Siwiecki M., Kowalski P., *Przeszukanie i zatrzymanie rzeczy w sprawach o cyberprzestępstwa. Udział specjalistów i biegłych w czynnościach procesowych*, „Kwartalnik Policyjny" 2021, t. 57, nr 2.
Szumiło-Kulczycka D., *Między ochroną prywatności a bezpieczeństwem – uwagi na tle orzecznictwa ETPCz i TSUE* [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017.
Wrona J., Zawadzka Z., *Cyberbezpieczeństwo w prawie własności intelektualnej* [w:] *Cyberbezpieczeństwo. Zarys wykładu*, red. C. Banasiński, Warszawa 2018.

Procedural surveillance of correspondence stored in the cloud computing

Abstract

The article attempts to analyze the process control of correspondence stored in virtual memory, i.e. in the so-called Cloud Computing. The study is an attempt to answer the question of how mobile devices and clouds are examined and what impact the law on privacy has on the implementation of procedural activities. The growing interest in cloud computing results in the emergence of many new legal problems, which translate into, among others, on the practice and operation of law enforcement agencies. First, the concept of „cloud computing" was discussed and the provisions on obtaining electronic evidence were analyzed. The independence of ICT systems from the functioning of a classic work environment based on a single workstation also allowed us to raise the question of the cross-border nature of services provided in the cloud. IT data transmitted via cloud computing can be saved on several devices located in different countries.

Key words: cloud computing, physical imaging, logical imaging, search, securing evidence

Elżbieta Żywucka-Kozłowska*
Rossana Broniecka**

Bezpieczeństwo osób nietrzeźwych w izbach wytrzeźwień. Technika cyfrowa jako instrument bezpieczeństwa

Streszczenie

Celem niniejszego opracowania jest próba przedstawienia problemu bezpieczeństwa człowieka w stanie nietrzeźwości w izbach wytrzeźwień. Osoby tam umieszczone mają zapewnioną opiekę medyczną. Zgodnie z przyjętymi regulacjami prawnymi w placówce takiej zatrudniony jest personel medyczny – lekarz lub felczer oraz pielęgniarz bądź ratownik medyczny. Mimo przyjętych procedur dochodzi do zagrożenia bezpieczeństwa osób nietrzeźwych, a także do zagrożenia bezpieczeństwa personelu tam pracującego.

Do izby wytrzeźwień trafiają osoby, których nietrzeźwość określa zawartość alkoholu powyżej 0,5 promila, które swoim zachowaniem zagrażają sobie bądź innym osobom, a także nietrzeźwi budzący zgorszenie w miejscu publicznym. Przyjęto zasadę, że nietrzeźwych, u których stężenie alkoholu jest równe lub wyższe niż 4 promile są odsyłani transportem medycznym do szpitala. Narzędziem wspierającym bezpieczeństwo osób przebywających w takich placówkach jest monitoring wizyjny, który umożliwia nie tylko bieżącą obserwację osób przebywających w izbach wytrzeźwień, lecz także odtworzenie nagrań w celu oceny zdarzeń w razie potrzeby.

Słowa kluczowe: izba wytrzeźwień, stan nietrzeźwości, technika cyfrowa, bezpieczeństwo

* Dr hab. Elżbieta Żywucka-Kozłowska, Wydział Prawa i Administracji, Katedra Postępowania Karnego i Prawa Karnego Wykonawczego, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: elzbieta.kozlowska@uwm.edu.pl, ORCID: 0000-0000-0002-6039-5580.
** Dr Rossana Broniecka, Wydział Prawa i Administracji, Katedra Postępowania Karnego i Prawa Karnego Wykonawczego, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: rossana.broniecka@uwm.edu.pl, ORCID: 0000-0001-7967-0143.

Według ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi „[...] organy samorządu terytorialnego w miastach liczących ponad 50 000 mieszkańców i organy powiatu mogą organizować i prowadzić izby wytrzeźwień”[1]. Są one przeznaczone przede wszystkim dla osób nietrzeźwych, których zachowania „[...] dają powód do zgorszenia w miejscu publicznym lub w zakładzie pracy, znajdują się w okolicznościach zagrażających ich życiu lub zdrowiu albo zagrażają życiu lub zdrowiu innych osób”[2]. Nie jest niczym odkrywczym, że stan nietrzeźwości stanowi jedną z przyczyn nie tylko przestępczości, lecz także zgonów osób, które wprowadziły się w taki stan. Izby wytrzeźwień na stałe wpisały się w polską rzeczywistość. Są miejscem szczególnym, bo zapewniają nietrzeźwym bezpieczeństwo w powszechnym znaczeniu tego terminu. Celem niniejszego opracowania jest próba przedstawienia problemu bezpieczeństwa człowieka w stanie nietrzeźwości w tym jednym, konkretnym miejscu.

Uzależnienia, w tym alkoholizm, prowadzą do trwałych zmian w ludzkim zachowaniu, a także powodują wiele innych skutków, w tym zdrowotnych, społecznych i prawnych. Problem uzależnienia jest obecny we wszystkich państwach współczesnego świata. Alkoholizm i narkomania zajmują wysoką pozycję w tym niechlubnym rankingu[3]. Przywołana w pierwszym zdaniu tego opracowania ustawa o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi jest podstawowym aktem prawnym dotyczącym profilaktyki przedmiotowego uzależnienia. Na podstawie tego aktu prawnego zostały wydane rozporządzenia:

1. Rozporządzenie Ministra Zdrowia z dnia 12 maja 2020 r. zmieniające rozporządzenie w sprawie funkcjonowania podmiotów leczniczych sprawujących opiekę nad uzależnionymi od alkoholu (Dz.U. 2020, poz. 850);

2. Rozporządzenie Ministra Zdrowia i Ministra Spraw Wewnętrznych i Administracji z dnia 28 grudnia 2018 r. w sprawie badań na zawartość alkoholu w organizmie (Dz.U. 2018, poz. 2472);

3. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 lipca 2019 r. zmieniające rozporządzenie w sprawie pomieszczeń przeznaczonych dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia, pokoi przejściowych, tymczasowych pomieszczeń przejściowych i policyjnych

1 Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi, t.j., Dz.U. 2002, nr 147, poz. 1231, z późn. zm., art. 39.

2 Ibidem, art. 40, ust. 1.

3 Dane statystyczne dotyczące spożycia alkoholu w Polsce zob. https://www.parpa.pl/index.php/badania-i-informacje-statystyczne/statystyki [dostęp: 2.01.2023].

izb dziecka, regulaminu pobytu w tych pomieszczeniach, pokojach i izbach oraz sposobu postępowania z zapisami obrazu z tych pomieszczeń, pokoi i izb (Dz.U. 2019, poz. 1341);

4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 26 września 2022 r. zmieniające rozporządzenie w sprawie badań lekarskich osób zatrzymanych przez Policję (Dz.U. 2022, poz. 2004).

Osoby zatrzymane w izbach wytrzeźwień[4] zgodnie z obowiązującymi przepisami mają zagwarantowane bezpieczeństwo, w tym osobiste, zdrowotne i sanitarne. W literaturze przedmiotu niekiedy osoby takie są określane jako pacjenci[5]. Mimo że w obowiązujących przepisach prawa dotyczących funkcjonowania izb wytrzeźwień nie występuje termin „pacjent", w literaturze medycznej zwraca się uwagę na różne aspekty krótkotrwałej izolacji w tego rodzaju placówkach[6]. Nie ma w tym niczego nowego, zwłaszcza że w praktyce wielu nietrzeźwych trafia do placówek medycznych nie tylko z przyczyn urazowych, lecz także z powodu ostrego zatrucia[7]. Leczenie takich pacjentów przebiega według przyjętych w medycynie procedur. W izbach wytrzeźwień osoby tam umieszczone mają zapewnioną opiekę medyczną. Zgodnie z przyjętymi regulacjami prawnymi w takiej placówce jest zatrudniony personel medyczny – lekarz lub felczer oraz pielęgniarz bądź ratownik medyczny[8]. Rozważania o bezpieczeństwie osób umieszczanych w izbach wytrzeźwień są obecne

4 Izby wytrzeźwień mają dziś inne nazewnictwo – o nowym nazewnictwie zdecydowały w ostatnich latach miejskie samorządy – np. Szczecińskie Centrum Profilaktyki Uzależnień czy Ośrodek dla Osób Nietrzeźwych w Poznaniu.

5 Zob. I. Paradowska, *Pacjenci płockiej izby wytrzeźwień*, „Notatki Płockie" 1989, nr 1; W. Bednarski, E. Rozmysl, J. Bertrandt, A, Klos, *Ocena sposobu żywienia osób bezdomnych, pacjentów Izby Wytrzeźwień w Warszawie – badania wstępne*, „Żywienie Człowieka i Metabolizm. Suplement" 2005, nr 1, cz. 2.

6 Zob. m.in.: C. Żaba, P. Świderski, Z. Żaba, D. Lorkiewicz-Muszyńska, *Zgony w izbie wytrzeźwień w Poznaniu*, „Archiwum Medycyny Sądowej i Kryminologii" 2009, t. 59, nr 2, s. 112–117; T. Brodziak, K. Kordel, C. Żaba, *Zgony w izbie wytrzeźwień – analiza przypadków sekcjonowanych w latach 1980–1991 w Zakładzie Medycyny Sądowej AM w Poznaniu ze szczególnym uwzględnieniem lekarskich pomyłek diagnostycznych*, „Postępy Medycyny Sądowej i Kryminologii" 1995, t. 2, s. 271–279.

7 Zob. m.in.: Z. Marek, *Nietrzeźwość wśród zmarłych z przyczyn chorobowych i gwałtownych*, „Archiwum Medycyny Sądowej i Kryminologii" 1988, t. 38, nr 4, s. 210–217; W.E. Erwin, D.B. Williams, W.A. Speir, *Delirium tremens*, „Southern Medical Journal" 1998, nr 5, s. 425–432; Z. Chodorowski, H. Kujawska, M. Wiśniewski, R. Ciechanowicz, *Wybrane aspekty kliniczne ostrego zatrucia alkoholem etylowym*, „Przegląd Lekarski" 2004, nr 4, s. 314–316.

8 Rozporządzenie Ministra Zdrowia z dnia 8 grudnia 2014 roku w sprawie izb wytrzeźwień i placówek wskazanych lub utworzonych przez jednostkę samorządu terytorialnego, Dz.U. 2022, poz. 2075.

w literaturze przedmiotu od wielu lat. Nie sposób w tym miejscu nie wskazać pracy Zbigniewa Kallausa, który opisał przypadek mężczyzny, który został przewieziony z izby wytrzeźwień do szpitala w stanie ciężkim, gdzie mimo reanimacji zmarł. Autor podkreśla nie tylko błędne rozpoznanie stanu zdrowia mężczyzny przez lekarza, który uznał, że ten może być zatrzymany w izbie wytrzeźwień, ale także wadliwe postępowanie drugiego lekarza (przejął dyżur) polegające na fiksacji chorego[9]. Przykład ten dowodzi, że mimo przyjętych procedur postępowania w tych placówkach, dochodzi do zagrożenia bezpieczeństwa nietrzeźwych. Z drugiej strony, istnieje inny problem – bezpieczeństwa personelu izb wytrzeźwień[10].

Spożywanie alkoholu ma długą tradycję w wielu współczesnych społeczeństwach. Grecy, Włosi czy Hiszpanie preferują wina, Niemcy, Czesi – piwo, Polacy mimo zmiany w wyborze rodzaju alkoholu, wybierają zarówno wino, piwo, jak i wódkę[11]. Mimo coraz powszechniejszych działań profilaktycznych (i terapeutycznych) problem alkoholizmu istnieje i nic nie wskazuje, żeby miał być wyeliminowanym z życia społecznego. Tytułowe izby wytrzeźwień (pozostajemy przy tym nazewnictwie) nie są placówkami medycznymi, nie świadczą usług medycznych, bo nie takie jest ich przeznaczenie. Zgodnie z obowiązującymi przepisami prawa (uprzednio wskazywanymi) wśród personelu takiej placówki są lekarze i średni personel medyczny. Zadaniem medyków jest ocena, czy doprowadzony kwalifikuje się do pobytu w izbie czy nie, co w praktyce oznacza przekazanie do placówki medycznej (szpitala). Przesłankami odmowy przyjęcia są m.in.: rany cięte, urazy głowy, złamania kończyć, zaburzenia rytmu serca, niewydolność oddechowa, zatrucie alkoholem, drgawki, utrata przytomności i wyniszczenie[12]. Do izby wytrzeźwień trafiają osoby, których nietrzeźwość określa zwartość alkoholu powyżej 0,5 promila i które swoim

9 Z. Kallaus, *Nadużycie władzy przez lekarza*, „Palestra" 1978, nr 11–12, s. 43–50.

10 Zob. m.in.: K. Frydrysiak, J. Ejdukiewicz, M. Grześkowiak, *Agresja pacjentów i ich bliskich wobec personelu szpitalnego oddziału ratunkowego*, „Anaesthesiology & Rescue Medicine/ Anestezjologia i Ratownictwo" 2016, nr 1; E. Rudnicka-Drożak, P. Misztal-Okońska, *Analiza struktury i częstości przyjęć pacjentów w stanie zatrucia alkoholem na przykładzie dwóch lubelskich szpitali*, „Alcoholism and Drug Addiction" 2014, nr 1; M. Kołpa, A. Grochowska, A. Gniadek, B. Jurkiewicz, *Pourazowe obrażenia czaszkowo-mózgowe u pacjentów w stanie nietrzeźwości, przyjmowanych doraźnie do szpitalnego oddziału ratunkowego*, „Medycyna Ogólna i Nauki o Zdrowiu" 2016, nr 1.

11 W świetle danych Eurostatu z roku 2014 w państwach UE nałogowo pije alkohol 27,8 mln osób – zob. https://hh24.pl/alkoholizm/ [dostęp: 6.01.2023].

12 E. Brzozowska, *Co się dzieje w izbach wytrzeźwień? Wielu mówi do zobaczenia i wraca*, https://www.medonet.pl/zdrowie/zdrowie-dla-kazdego,co-sie-dzieje-w-izbach-wytrzezwien--wielu-mowi-do-zobaczenia-i-wraca,artykul,83285381.html [dostęp: 6.01.2023].

zachowaniem zagrażają sobie bądź innym osobom, a także nietrzeźwi budzący zgorszenie w miejscu publicznym. Przyjęto zasadę, że nietrzeźwych, u których stężenie alkoholu jest równe lub wyższe niż 4 promile są odsyłani transportem medycznym do szpitala[13]. Od 1956 roku, kiedy to powstały w Polsce pierwsze izby wytrzeźwień, zdecydowanie zmieniły się zarówno warunki pobytu, jak i bezpieczeństwo doprowadzonych. Narzędziem wspierającym bezpieczeństwo osób przebywających w takich placówkach jest monitoring wizyjny[14] – „[...] zamknięte pomieszczenie przeznaczone do izolacji wyposaża się w instalację monitoringu umożliwiającą stały nadzór nad osobą w nim umieszczoną oraz kontrolę wykonania czynności związanych z tym środkiem przymusu bezpośredniego"[15]. W dalszej części tego przepisu wskazano, że monitoring „[...] pomieszczeń lub ich części przeznaczonych do celów sanitarnohigienicznych jest przekazywany w sposób uniemożliwiający ukazywanie intymnych części ciała ludzkiego oraz intymnych czynności fizjologicznych"[16]. Niezwykle istotny jest zapis ustępu 14 rzeczonej ustawy o pisemnym upoważnieniu osób, które utrwalają i przetwarzają dane z monitoringu. Ustawodawca nakazuje tym podmiotom zachowanie tych danych w poufności. Niezwykle ważny z punktu widzenia bezpieczeństwa jest przepis art. 42 ust. 15 przywołanej ustawy, który stanowi: „Zapis monitoringu jest przechowywany przez okres co najmniej 30 dni, nie dłużej jednak niż 60 dni od dnia jego zarejestrowania, o ile nie zostanie on zabezpieczony jako dowód w sprawie w przypadku toczącego się postępowania. Po upływie terminu przechowywania zapis usuwa się w sposób uniemożliwiający jego odzyskanie. Z usunięcia zapisu sporządza się protokół, w którym należy wskazać datę tej czynności oraz imię i nazwisko osoby, która dokonała usunięcia. Dopuszcza się niszczenie zapisu na urządzeniu monitorującym przez jego automatyczne nadpisanie w przypadku, gdy warunki techniczne tego urządzenia umożliwiają przechowywanie zapisu przez okres, o którym mowa w zdaniu pierwszym"[17]. Przechowywanie danych z monitoringu przez nie mniej niż 30 dni stanowi obowiązek ustawowy. Dane takie pozwalają na odtworzenie zdarzeń w określonym przedziale czasowym, a mającym znaczenie w razie zdarzeń ważnych dla oceny prawnokarnej. W literaturze przedmiotu, co już podkreślano, zgony

13 Ibidem.
14 Ustawa z dnia 26 października 1982 r. o wychowaniu w trzeźwości..., art. 42.
15 Ibidem, art. 42, ust. 12.
16 Ibidem, art. 42, ust. 13.
17 Ibidem, ust. 15.

w izbach wytrzeźwień nie są częste, ale się zdarzają i wymagają wyjaśnienia zarówno przyczyny, jak i okoliczności śmierci nietrzeźwego przebywającego w takiej placówce. Czesław Żaba, Paweł Świderski, Zbigniew Żaba i Dorota Lorkiewicz-Muszyńska podkreślają, że „[...] przypadki zgonów związanych z pobytem w izbie wytrzeźwień są wprawdzie na przestrzeni lat stosunkowo rzadkie i niezbyt często podejmowane w piśmiennictwie, jednak z wielu przyczyn wciąż budzą kontrowersje, a ich liczba pomimo upływu lat nie spada. Ocena stanu zdrowia człowieka w stanie upojenia alkoholowego nie jest rzeczą łatwą, wymaga dużego doświadczenia od lekarza i jego odporności na nierzadko wulgarne i agresywne zachowanie pacjenta. Wielu z tych zgonów nie można było zapobiec nawet przy optymalnym postępowaniu lekarskim, jednakże wciąż znacząca pozostaje liczba przypadków zaniedbania, zaniechania leczenia szpitalnego czy błędów diagnostycznych”[18]. W tym miejscu warto przedstawić przypadki zgonów w takich miejscach, o których informuje Policja. W Rzeszowie 26 sierpnia 2009 roku około godziny 7.15 policjanci zostali poinformowani przez obsługę izby wytrzeźwień o zgonie mężczyzny przebywającego tam do wytrzeźwienia. Zabezpieczono dokumentację dotyczącą zmarłego oraz zapis z kamer monitorujących pomieszczenie, w którym przebywał mężczyzna[19]. W 2021 roku we wrocławskiej izbie wytrzeźwień zmarł 25-letni mężczyzna. Postępowanie w tej sprawie prowadzi Prokuratura Okręgowa w Szczecinie. Dziewięciu osobom przedstawiono zarzuty pobicia ze skutkiem śmiertelnym, znęcania się nad osobą zatrzymaną, narażenia pokrzywdzonego na bezpośrednie niebezpieczeństwo utraty zdrowia, podżegania do utrudniania postępowania karnego i poświadczania nieprawdy w dokumentacji medycznej dotyczącej pobytu mężczyzny zatrzymanego do wytrzeźwienia[20]. Monitoring wizyjny jest tym narzędziem cyfrowym, które umożliwia odtworzenie nagrań w celu obiektywnej oceny zdarzeń. Bezpieczeństwo osób przebywających w tytułowych placówkach pozostaje w zainteresowaniu nie tylko organów prowadzących, kontrolujących, lecz także Rzecznika Praw Obywatelskich. W raporcie Krajowego Mechanizmu Prewencji Tortur z wizytacji izby wytrzeźwień działającej w Ośrodku Wczesnej Interwencji dla

18 C. Żaba, P. Świderski, Z. Żaba, D. Lorkiewicz-Muszyńska, op. cit., s. 116.

19 *Zmarł pensjonariusz izby wytrzeźwień*, https://podkarpacka.policja.gov.pl/rze/komendy-policji/kmp-rzeszow/wydarzenia/36100,Zmarl-pensjonariusz-Izby-Wytrzezwien.html [dostęp: 6.01.2023].

20 *Śmierć 25-latka w izbie wytrzeźwień. Dziewięć osób z zarzutami*, https://www.rmf24.pl/fakty/polska/news-smierc-25-latka-w-izbie-wytrzezwien-dziewiec-osob-z-zarzutam,nId,5570170#crp_state=1 [dostęp: 6.01.2023].

Osób z Problemem Alkoholowym i ich Rodzin w Lublinie z 25 sierpnia 2022 roku wskazano, że w wizytowanej izbie dostrzeżono pewne braki w dokumentowaniu obrażeń ciała osób przyjmowanych do wytrzeźwienia, co wynika wprost z protokołu stambulskiego[21]. Niezmiernie ważne w tym kontekście jest fotograficzne dokumentowanie stwierdzonych obrażeń, ale za zgodą osoby zatrzymanej. Wskazanie zgody na taką czynność nie wydaje się trafne, przede wszystkim z jednego powodu – nietrzeźwości badanego, u którego, czego nie trzeba wyjaśniać, stan taki powoduje zakłócenia czynności psychicznych. Zgoda wyrażona w stanie nietrzeźwości jest wątpliwa na gruncie prawa. Z tego też względu monitoring wizyjny jest szczególnie istotny, umożliwia bowiem ustalenie zachowania człowieka, ale też daje szansę na utrwalenie obrazu obrażeń ciała, jeżeli są w odkrytych partiach ciała. Wydaje się, że jeżeli regulacja krajowa przewiduje monitorowanie pomieszczeń dla doprowadzonych do izby wytrzeźwień, to należy rozważyć zapis o cyfrowym dokumentowaniu zarówno obrażeń ciała, jak i przedmiotów zatrzymanego zabezpieczanych w depozycie. Trzeba także podkreślić, że Polska jest stroną konwencji w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania przyjętej przez Zgromadzenie Ogólne Narodów Zjednoczonych 10 grudnia 1984 roku[22].

Narzędzia cyfrowe na stałe wpisały się w rzeczywistość społeczną, w wielu miejscach publicznych znajdują się kamery, co w istotny sposób przyczynia się do poprawy bezpieczeństwa. Monitoring w izbach wytrzeźwień jest nie tylko prawnie uregulowany, co wyżej wskazano, lecz także – w naszym przekonaniu – konieczny. Techniczne wsparcie bezpieczeństwa wymaga profesjonalizmu personelu, co nie zawsze ma miejsce. Przykładem może być samobójstwo doprowadzonego do wytrzeźwienia 46-letniego mężczyzny w Tychach w 2011 roku. Z dostępnych materiałów wynika, że powiesił się na jednorazowym prześcieradle, a sala, w której przebywał, była monitorowana, ale personel nie podjął interwencji. Zabezpieczone nagrania z monitoringu stały się dowodem w sprawie[23]. Rok po tym zdarzeniu Rzecznik Praw Obywatelskich w wystąpieniu

21 *Protokół stambulski. Podręcznik skutecznego badania i dokumentowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania*, Genewa–Nowy Jork 2004, https://bip.brpo.gov.pl/sites/default/files/protokol_stambulski_fin.pdf [dostęp: 7.01.2023].

22 Konwencja w sprawie zakazu stosowania tortur oraz innego okrutnego, nieludzkiego lub poniżającego traktowania albo karania, przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 10 grudnia 1984 r., Dz.U. 1989, nr 63, poz. 378.

23 *Powiesił się w izbie wytrzeźwień*, TVN24Polska, 14 marca 2011, https://tvn24.pl/polska/powiesil-sie-w-izbie-wytrzezwien-ra164598-3517239 [dostęp: 7.01.2023].

podkreślił, że „[...] nie wzbudza wątpliwości fakt, iż monitorowanie tych pomieszczeń przyczynia się do poprawy bezpieczeństwa i zapobiega występowaniu nadzwyczajnych wypadków. Jednak z drugiej strony, rozwiązanie to wiąże się z ograniczeniem prawa do prywatności [...] przypadki monitorowania pacjentów podczas rozbierania się lub badania lekarskiego (a takie Krajowy Mechanizm Prewencji zauważył podczas wizytacji niektórych izb) bezspornie są naruszeniem godności ludzkiej”[24]. Nie można w tym miejscu nie pochylić się nad zdaniem Rzecznika Praw Obywatelskich dotyczącym naruszenia godności ludzkiej polegającym na monitorowaniu (wizyjnym) badania lekarskiego oraz rozbierania. Trudno nie zgodzić się z tą tezą. Z drugiej strony, co przedstawiono wyżej, monitoring niejednokrotnie staje się materiałem dowodowym w sprawach, które zostały wszczęte przez organy ścigania w związku ze śmiercią doprowadzonego do izby wytrzeźwień. Postępowania takie dotyczą zarówno samobójstw, jak i pobić w związku z przekroczeniem uprawnień przez funkcjonariuszy Policji i personel tych placówek. Nie sposób nie dodać, że monitoring jest narzędziem, które pozwala odtworzyć ostatnie chwile zmarłych w izbie wytrzeźwień osób doprowadzonych. Marcin Kruk opisał przypadek zgonu mężczyzny doprowadzonego do izby wytrzeźwień, gdzie zmarł: „[...] ze wstępnych ustaleń prokuratury wynika, że podczas transportu do izby wytrzeźwień 52-latek zaczął czuć się źle. Z radiowozu do budynku WrOPON-u przewieziono go na wózku i od razu rozpoczęto akcję ratunkową. Prowadził ją lekarz izby, zostało wezwane pogotowie ratunkowe, ale resuscytacja oraz użycie defibrylatora nie pozwoliły uratować życia człowieka. – Lekarz w protokole zgonu stwierdził ostrą niewydolność krążeniowo-oddechową. Prokurator jeszcze na miejscu przeprowadził oględziny zewnętrzne ciała. Nie stwierdzono żadnych zasinień, obrażeń, zadrapań. Ciało skierowano na sekcję zwłok do Zakładu Medycyny Sądowej we Wrocławiu – mówi Małgorzata Dziewońska. Wyniki sekcji jeszcze nie są znane […]. Prokuratura zabezpieczyła monitoring i przesłuchała bezpośrednich świadków zdarzenia, lekarza i pracowników WrOPON-u, a także pracowników ochrony z dworca”[25]. W Koszalinie popełnił samobójstwo mężczyzna doprowadzony do placówki w stanie nietrzeźwości. Z oświadczenia rzecznika Prokuratury Okręgowej w Koszalinie wynika, że

24 *Monitoring w izbach wytrzeźwień – wystąpienie RPO*, 13.09.2012, https://panoptykon.org/wiadomosc/monitoring-w-izbach-wytrzezwien-wystapienie-rpo [dostęp: 7.01.2023].

25 M. Kruk, *Kolejna śmierć w izbie wytrzeźwień. Wrocławska prokuratura prowadzi śledztwo*, 10 stycznia 2022, https://gazetawroclawska.pl/kolejna-smierc-w-izbie-wytrzezwien-wroclawska-prokuratura-prowadzi-sledztwo/ar/c1-15990289 [dostęp: 8.01.2023].

mimo monitoringu pomieszczeń nagrania nie były zapisywane, a samo urządzenie było wykorzystywane wyłącznie do obserwacji[26]. W 2012 roku popełnił samobójstwo mężczyzna, którego doprowadzono do izby wytrzeźwień. „W sali przebywał sam. Kiedy przywieziono kolejnego nietrzeźwego, zauważono Artura M. wiszącego na okiennej kracie. Mimo reanimacji mężczyzny nie udało się uratować. Zajście zarejestrowała kamera. Pomieszczenia w izbie są monitorowane i widać jak Artur M. popełnia samobójstwo. Wszystko trwało około 5 minut, obraz podczas zdarzenia był przekazywany na monitor w pomieszczeniu obsługi, mimo to nikt tego nie zauważył"[27]. W tej sprawie pracownicy placówki zostali oskarżeni o niedopełnienie obowiązków. W piśmiennictwie podkreśla się, że osoby nietrzeźwe często deklarują myśli samobójcze, a także popełniają samobójstwa[28]. Związek nietrzeźwości z samobójstwem (dokonanym czy usiłowanym) znany jest od dawna, co potwierdzają statystyki policyjne. Z tego też względu monitoring wizyjny w izbach wytrzeźwień jest niezwykle ważny w zapewnieniu bezpieczeństwa osób tam doprowadzonych.

Bibliografia

Bednarski W., Rozmysl E., Bertrandt J., Klos A., *Ocena sposobu żywienia osób bezdomnych, pacjentów Izby Wytrzeźwień w Warszawie – badania wstępne*, „Żywienie Człowieka i Metabolizm. Suplement" 2005, nr 1, cz. 2.

Brodziak T., Kordel K., Żaba C., *Zgony w izbie wytrzeźwień – analiza przypadków sekcjonowanych w latach 1980–1991 w Zakładzie Medycyny Sądowej AM w Poznaniu ze szczególnym uwzględnieniem lekarskich pomyłek diagnostycznych*, „Postępy Medycyny Sądowej i Kryminologii" 1995, t. 2.

Chodorowski Z., Kujawska H., Wiśniewski M., Ciechanowicz R., *Wybrane aspekty kliniczne ostrego zatrucia alkoholem etylowym*, „Przegląd Lekarski" 2004, nr 4.

Erwin W.E., Williams D.B., Speir W.A., *Delirium tremens*, „Southern Medical Journal" 1998, nr 5.

Marek Z., *Nietrzeźwość wśród zmarłych z przyczyn chorobowych i gwałtownych*, „Archiwum Medycyny Sądowej i Kryminologii" 1988, t. 38, nr 4.

Frydrysiak K., Ejdukiewicz J., Grześkowiak M., *Agresja pacjentów i ich bliskich wobec personelu Szpitalnego Oddziału Ratunkowego*, „Anaesthesiology & Rescue Medicine/Anestezjologia i Ratownictwo" 2016, nr 1.

Kallaus Z., *Nadużycie władzy przez lekarza*, „Palestra" 1978, nr 11–12.

26 *Samobójstwo w izbie wytrzeźwień. Monitoring nie pomoże*, 19.02.2014, https://szczecin.wyborcza.pl/szczecin/7,34939,15489313,samobojstwo-w-izbie-wytrzezwien-monitoring-nie-pomoze.html [dostęp: 8.01.2023].

27 *Popełnił samobójstwo w izbie wytrzeźwień*, 22.11.2012, https://radio.opole.pl/100,83268,wiadomosci-z-regionu&dtx=&szukaj=&go=morelist&s=5 [dostęp: 8.01.2023].

28 Na ten temat zob. m.in.: A. Młodożeniec, *Ocena klinicznych czynników ryzyka samobójstwa*, „Suicydologia" 2008, nr 4, s. 20–28; W. Sołtys i in., *Deklaracje suicydialne pod wpływem alkoholu – postępowanie w warunkach psychiatrycznej izby przyjęć. Doniesienie wstępne*, „Psychiatria i Psychologia Kliniczna" 2012, nr 1, s. 34–39.

Kołpa M., Grochowska A., Gniadek A., Jurkiewicz B., *Pourazowe obrażenia czaszkowo-mózgowe u pacjentów w stanie nietrzeźwości, przyjmowanych doraźnie do szpitalnego oddziału ratunkowego*, „Medycyna Ogólna i Nauki o Zdrowiu" 2016, nr 1.
Młodożeniec A., *Ocena klinicznych czynników ryzyka samobójstwa*, „Suicydologia" 2008, nr 4.
Paradowska I., *Pacjenci płockiej izby wytrzeźwień*, „Notatki Płockie" 1989, nr 1.
Rudnicka-Drożak E., Misztal-Okońska P., *Analiza struktury i częstości przyjęć pacjentów w stanie zatrucia alkoholem na przykładzie dwóch lubelskich szpitali*, „Alcoholism and Drug Addiction" 2014, nr 1.
Sołtys W. i in., *Deklaracje suicydialne pod wpływem alkoholu – postępowanie w warunkach psychiatrycznej izby przyjęć. Doniesienie wstępne*, „Psychiatria i Psychologia Kliniczna" 2012, nr 1.
Żaba C., Świderski P., Żaba Z., Lorkiewicz-Muszyńska D., *Zgony w izbie wytrzeźwień w Poznaniu*, „Archiwum Medycyny Sądowej i Kryminologii" 2009, t. 59, nr 2.

Safety of the alcoholic intoxicated in the sobering chamber. Digital technique as a safety instrument

Abstract

The aim of the elaboration is an attempt to threaten the safety of an alcoholic intoxicated person in sobering chamber. In accordance with the legal regulations adopted in this regard, medical staff is employed in such a facility – a doctor or feldsher and a nurse or paramedic. However, despite the procedures adopted in such facilities, there is a threat to the safety of intoxicated persons, as well as to the safety of the staff working there.

The sobering chamber admits people whose intoxication determines the alcohol content above 0.5 per mille and whose influence affects themselves or otherwise, as well as intoxicated persons causing scandal in a public place. Rules have also been adopted that intoxicated people with alcohol equal to or higher than 4 per mille are referred to medical transport for care. The support of the safety of people staying in such facilities is video monitoring, which allows not only constant observation of people staying in sobering stations, but also but also playback of recordings for the purpose of evaluating events and their reconstruction.

Key words: sobering chamber, state of intoxication, digital technology, safety

Paulina Krawczyk*
Jarosław Wiśnicki**

Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022

Abstract

In this article, we attempt to identify Russia's social-impact operations in the context of information operations conducted by the Russian Federation during 2022 in the war against Ukraine. The need to undertake the analysis of the creation and proliferation of information threats, as a result of Russia's actions in the ongoing conflict, is dictated by the growing impact of communication processes on global security. This article discusses the impact and role of mass media on the shaping of people's minds, by exposing the mechanisms behind the formation of public opinion.

Key words: information warfare, media, information operations, disinformation

* Paulina Krawczyk, Faculty of National Security, War Studies Academy, Academic Centre for Cyber Security Policy, e-mail: p.krawczyk@akademia.mil.pl.
** Lt Col Jarosław Wiśnicki, Territorial Defence Forces Command, e-mail: jar.wisnicki@gmail.com.

Introduction

The purpose of this article is to attempt to identify the social-impact operations in the context of information operations conducted by the Russian Federation in 2022 in the war against Ukraine. The study outlines the impact of trends in the creation of information threats acting as determinants of social threats. The analysis of the emergence of information threats, taking into account the creation and distribution of information, both via direct messages and with the use of intelligence techniques, constitutes an important part of the article. The authors, when selecting the topic to be discussed in the paper, referred primarily to the up-to-datedness of the problem under analysis. This is because Russian information operations represent the modern use of armed forces in accomplishing military objectives. Actions targeted at Ukraine reflect the practical implementation of Russia's assumptions.

Communication space as an area of information operations

Nowadays, in the times of efficient and rapidly-acting media, the range of opportunities they offer, when it comes to exerting social impact, are being intensively exploited. Nowadays, it is not the courts that determine who is guilty – public opinion does so, being judgemental and passing sentence every moment. A synthetic expression of public opinion, in the context of Russia's actions in the war in Ukraine, is the way they are presented. This means how they appear, in overall terms, to the public. Therefore, it appears of the utmost importance to investigate, in scientific terms, the appropriateness of selecting tools and techniques to exert social impact in the formation of public opinion.

In doing so, the thesis that mass media are a powerful weapon used by many circles (not only by authorities) to direct and shape public opinion should be considered the starting point. Public opinion means views, attitudes and assessments (judgements), concerning some specific current subject (value) or some specific person, and the way he/she behaves, formulated and communicated to one another by members of the public, focused on the value or the person being subjected to judgement. It is, therefore, quite easy to understand why the mass media are so often used to shape public opinion, and its creators may include: state bodies, services dedicated to implementing social impact operations, non-state actors, social activists, and institutions

involved in the transmission of information with broad access to social groups (press agencies, newspapers, television, radio, and the Internet)[1].

When dealing with the issue in question, we need to make it clear that it is a well-known regularity in the development of the art of war that exploring the specific features of future conflicts requires analysing and evaluating future events. Only then, based on the results obtained, can any specific conclusions for the future be formulated. This is of particular importance as regards the ongoing war, in which information operations play a vital role. It should be stressed that the present situation has been challenging to define for both the parties involved in the conflict and the international community, and has exposed the dynamics with which information spreads and, in particular, the impact it has on international public opinion. Therefore, it should be assumed that the psychological dimensions of the conflict are as important as the physical ones. The conflict is a battle of intent which is fought both in people's minds and on the battlefield and is a conflict of clashing forces. These can be political (ideological), economic, cultural, religious and military forces, i.e., all those aspects of social life that, by intertwining, exert influence on people's will. Skilfully „whispered" warfare shapes and influences individual and group beliefs and behaviours, contributing to the accomplishment of the tactical or strategic goals of the aggressor.

Before proceeding with a detailed discussion, the authors will outline Russian military thoughts from the angle of information operations, along with referring to the main Russian ideologist of neo-imperialism, Aleksandr Dugin, who made a significant contribution to developing new-generation warfare strategies. The adviser to Putin and his generals, by referring to information operations, argues that the effective conduction of such operations makes it possible to secure victory in a conflict without establishing numerical superiority beforehand, even on a classic battlefield. This component of the adopted strategy should be viewed as the most original and as the one requiring particular attention. One of its manifestations includes actions aimed at distorting public order by destabilising the internal situation. Bringing about such a state causes social tensions to escalate, which results in social atomisation and polarisation. As a consequence, decision-making processes are disrupted, causing destabilisation of international cooperation; a potential adversary loses its position as a responsible and credible partner in

1 J. Braun, *Potęga czwartej władzy. Media, rynek, społeczeństwo*, Warszawa 2005, p. 77.

the international arena, especially in the economic or energy context, or in terms of other issues that are important from Moscow's point of view. Another, and often parallel, activity is to promote a negative image of an adversary, depreciating its authorities, antagonising societies, and portraying it as an aggressor that is intolerant, xenophobic, fascist, etc. Yet another method is to create the impression that Russia is more dangerous than it is, thus discouraging the West from escalating or becoming militarily involved in conflicts.

A confirmation for the discussed course of action can be found in the concept of new-generation warfare announced by General Valery Gerasimov, the Chief of General Staff of the Russian Army. The document was officially announced on 25 January 2014 at the Academy of Military Sciences, and its detailed discussion was published on 27 February 2013[2]. The following year, an amendment was published to the War Doctrine of the Russian Federation, signed by President Vladimir Putin on 26 December 2014. The doctrine has „egitimised" hybrid warfare, which implies the need to take into consideration a possible subliminal aggression scenario. The doctrine in question also recognises the emerging trend of shifting the dangers and threats of war to the information space. Furthermore, the doctrine enumerates the features and characteristics of modern military conflicts by referring to the complex use of military, political, economic and information power as well as other measures of a non-military nature, by exploiting the potential of public protests and forces conducting special operations. Attention is drawn to the fact that the impact on an adversary will be exerted across its entire territory, in the global information space.

Disinformation operations

Acquiring newer and newer interfaces requires increasingly greater efficiency. In facing this challenge, artificial intelligence is one of the solutions that may prove useful. Its use in the fabrication of fake news is becoming increasingly important. Simply put, bots are programs designed to allow a machine to perform certain actions at the command of a human. Their functioning is fully automated and based on algorithms. These algorithms,

2 P. Mickiewicz, *Rosyjska myśl strategiczna i potencjał militarny w XXI wieku* [in:] *Rosyjska myśl wojskowa i jej przeobrażenia w kontekście zmiany zagrożeń i sposobów wykorzystania potencjału militarnego w XXI w.*, ed. D. Kasprzycki, Warszawa 2018, p. 196.

for example, select content that matches our expectations and provides us with specific advertisements or webpages. They are becoming an increasingly important player in election campaigns by imitating people and influencing their behaviour. Social networking sites constitute a specific domain within which they operate. Being perfectly capable of processing large amounts of information in a short period, they are ideal tools for manipulation. There is an ever-increasing spread of false information that inspires ordinary people to disseminate misinformation. This is how people get locked in information bubbles and their views, which are not always correct, become reinforced. This mechanism is very likely to accelerate with the emergence of specialised bots (chatbots) dedicated to human-machine communication. David A. Broniatowski, Director of the GW Institute for Data, Democracy and Politics, argues that „bots can make the platforms' algorithms assume that automated content is more popular than it is, which can lead to platforms actually prioritising disinformation and spreading it to even larger audiences"[3]. So, numerous factors seem to suggest that the race between the makers of social-impact tools intended to manipulate people more effectively is well underway.

An extremely significant issue concerning disinformation is possessing knowledge of an adversary, and the methods and tools that an adversary employs in information warfare. It should be stressed that humans are the entities most vulnerable to disinformation. Disinformation mechanisms influence the selection of appropriate methods and techniques to exert impact on people's attitudes and behaviours. In the contemporary world, there is a strive towards a means of communication that is based on a combination of all elements, including written texts, images and sounds, and these possibilities are provided by modern means of communication, i.e., television, press, radio and the Internet. This is also connected with the capabilities of the human brain to receive information and content[4].

The media occupy an undoubtedly important place in the formation of public opinion, which is an extremely significant factor in the development of society. One of the disinformation methods is manipulation which, in the mass media, is a form of influencing an audience to make them carry out actions

3 *Boty głównymi roznosicielami dezinformacji w pandemii*, oprac. N. Makarewicz, https://www.rmf24.pl/raporty/raport-koronawirus-z-chin/polska/news-boty-glownymi-roznosicielami-dezinformacji-w-pandemii,nId,5285963#crp_state=1 [access: 16.06.2021].
4 G. Nowacki, *Rola technologii informacyjno-telekomunikacyjnych w działaniach psychologicznych*, „Nierówności Społeczne a Wzrost Gospodarczy" 2017, no. 4, p. 280.

which correspond to the needs of the manipulator, without the audience even being aware. People are usually not interested in whether any actions taken by the recipient of the information bring benefits to the sender or whether they have any different effects. The individuals or groups of people being manipulated are not aware of how the influence is being exerted. The sender usually seeks to have some personal, economic or political gain at the expense of those subjected to manipulation. As a result of such activities, the person subjected to manipulation is most often unaware of it and, when this is made clear, he/she tends to strongly deny acting in an uncontrolled manner. The way recipients approach information which is spread via the media, and their conviction of making their decisions independently makes them extremely resistant to persuasion and to any attempts to show them the real situation. For this reason, it is necessary to equip institutions with indispensable tools and to educate citizens on how to effectively defend themselves against manipulation[5].

The media not only contribute to the formation of certain opinions but can also stop their dissemination. Opinions can be easily measured, which makes them an important tool in the hands of the media as the media have the adequate resources to effectively encourage individuals to express opinions or, to the contrary, not to express them on a given topic[6].

Intelligence activities and direct communication

The development of the Internet has made it possible for users to access not only various sources of information but also to create information, bypassing traditional information providers operating with the use of classic means of social communication. A special role in this process is played by various types of social networking sites. This method of gathering and disseminating information has also contributed to the creation of sources of information which contradict the truth or public morality, or which infringe upon personal rights. The narrative, addressed to a broad range of Russian audiences, was based on depicting a false image of reality, and information concerning Russia's attack on Ukraine was shaped to present it as special operations

5 Ibidem, p. 279.
6 E. Maigret, *Socjologia komunikacji i mediów*, Warszawa 2012, p. 322.

aimed at the alleged disarmament of Ukraine and the restoration of order in the country, as well as giving new shape to the socio-political and economic community that allegedly existed between Russia and Ukraine. Statements made in the media by numerous experts, who emphasised during debates that the ongoing operation would not aggravate relations between Russian and Ukrainian societies, can be seen as another example of direct communication. The displaying of information that is supposed to give credence to untrue theses is mainly carried out via special services and military intelligence, which has increased the number of people appointed as journalists in eastern Ukraine and the bordering regions. They were made responsible for producing videos and photographs showing alleged provocations, although they often participated in them themselves.

By implementing their security policies, states are constantly facing challenges connected with securing their own information needs. Tasks of this type are mainly carried out by special services, which in addition to information acquisition, are involved in information disruption carried out in both offensive and defensive operations. Disruption is a specific action type requiring the conduction of operational activities. This is a complex process that, in addition to an information supply, requires the involvement of an influence agentry[7].

Information warfare and information operations are conducted in the information space. They aim to damage resources and systems, including IT ones, and to undermine the political and social systems and weaken the psychological impact on society. Of note is the fact that each country has adequate resources responsible for information warfare. The situation created in Ukraine is often different than the one commonly portrayed. Both sides resort to disinformation and fight their information warfare.

Information provided by the Ukrainian government and administration, as well as the media using examples of disinformation, also constitute examples of direct communication in the Russian-Ukrainian war. In addition, the information provided directly by the Americans sometimes differs from that disseminated by Ukraine, for example, regarding the number of Russian soldiers killed. Ukraine's primary objective connected with presenting this figure as larger than appears is to boost the morale of its troops. A study conducted by experts dealing with social psychology revealed a difference

7 A. Żebrowski, *Agentura wpływu uczestnikiem walki informacyjnej*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, no. 1, p. 61.

between the motivation and will of people who are faced with certain tasks and provided with information that the tasks were solvable, on the one hand, and those who have no such knowledge, on the other. This also holds true when it comes to the attitude of soldiers and civilians who help the military. The developed narrative of the incapacity of the Russian troops, coupled with information about the great successes attained by Ukrainian troops, is intended to influence Ukrainian minds and sustain motivation. One of the underlying tools of information warfare is intelligence services gathering necessary information about an adversary and conducting information warfare. As can be expected, intelligence activities should be supported by propaganda, which in turn can obtain a lot of valuable information from intelligence services. The most effective diversion method used by intelligence services is to inspire erroneous decisions on the part of the adversary and then exploit their consequences. This is a specific kind of manipulation, the essence of which is the covert steering of the adversary towards self-destruction[8].

Steering channels influencing an adversary's structure in information warfare processes can be divided into 1) information channels – collecting and passing relevant information to the headquarters, including, primarily, information about an adversary and its environment; and 2) steering and diversion channels – influencing an adversary's system, inspiring some decisions and actions while blocking others.

Both types can be covert or overt, with examples including an intelligence agent acting as a covert channel and a military attaché acting officially as an overt channel.

Along with destroying an adversary's system, information warfare is also about defending one's system against destructive impacts. Such defensive actions in information warfare can be perceived in the same way as offensive actions, except that their object is not an adversary's entire system, but certain organs conducting information warfare. For instance, on the national scale, defensive information warfare is conducted by counterintelligence which establishes its steering channels of all the aforementioned types, primarily in an adversary's intelligence organs (activities of this type can be referred to as offensive counterintelligence), as well as in all organisations which cooperate or may cooperate with an adversary's intelligence. The basis of countering an adversary's intelligence is the identification

8 J. Kosecki, *Elementy wojny informacyjnej*, http://autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf [access: 20.06.2022].

of its channels. Steering and diversion channels can be traced by observing their operations and consequence, while purely information channels can be recognised indirectly, e.g., by observing an adversary's decisions and actions taken based on the information supplied via these channels. It is generally much easier to uncover the steering and diversion channels than purely information channels; therefore, in well-organised information warfare bodies, these channels should be separated[9].

One of the underlying objectives of non-military hybrid conflicts is to influence people's way of thinking and to primarily manipulate those who are responsible for making key state decisions. The analysis of the events taking place in Ukraine since the beginning of the war has shown that, among the non-military methods of war-making, one can distinguish the increased activity of special forces, whose task is to collect information and to develop intelligence and sabotage networks to conduct operations in the territory of an attacked state. In addition, among the direct methods of conducting information warfare, the following can be included: the use of economic pressure, diplomatic actions, and offensive actions in cyberspace, carried out by the aggressor's special services or groups of hackers and hacktivists associated with these forces[10].

Exerting information-psychological influence is a procedure through which direct information is deliberately spread to affect the functioning and development of an information environment. The purpose of information operations conducted during the war may be, for example, to convince society that the interests of an enemy state are also their interests, by undermining trust in the state authorities and even by escalating tension and engaging social groups in the conflict[11].

Conclusions

Non-contact warfare has been, still is, and will continue to be, a component of interdisciplinary combinations of pervading layers and dependencies. This makes impact operations even more imperceptible. This type of warfare

9 Ibidem.
10 M. Wrzosek, S. Markiewicz, Z. Modrzejewski, *Informacyjny wymiar wojny hybrydowej*, Warszawa 2019, p. 96.
11 Ibidem, p. 99.

has evolved over the years, and so has the broadly perceived military instrumentation that includes combat tactics, means of war-making or organisation of the military. The influencing of people's minds produces greater effects than could previously be assumed, in particular when a civilian population and the armed forces of an opposing side have not been prepared for facing such factors. In times of conflict and war, psychological factors become particularly important, both among the direct participants and the population outside the conflict-affected area, due to sudden changes in circumstances and behaviours. This type of war-making will be used more and more frequently in the future, and social impact operations will be increasingly important, becoming an intrinsic element of cognitive warfare.

Bibliography

Boty głównymi roznosicielami dezinformacji w pandemii, oprac. N. Makarewicz, https://www.rmf24.pl/raporty/raport-koronawirus-z-chin/polska/news-boty-glownymi-roznosicielami-dezinformacji-w-pandemii,nId,5285963#crp_state=1 [access: 16.06.2021].

Braun J., *Potęga czwartej władzy. Media*, *rynek*, *społeczeństwo*, Warszawa 2005.

Kosecki J., *Elementy wojny informacyjnej*, http://autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf [access: 20.06.2022].

Maigret E., *Socjologia komunikacji i mediów*, Warszawa 2012.

Mickiewicz P., *Rosyjska myśl strategiczna i potencjał militarny w XXI wieku* [in:] *Rosyjska myśl wojskowa i jej przeobrażenia w kontekście zmiany zagrożeń i sposobów wykorzystania potencjału militarnego w XXI w.*, ed. D. Kasprzycki, Warszawa 2018.

Nowacki G., *Rola technologii informacyjno-telekomunikacyjnych w działaniach psychologicznych*, „Nierówności Społeczne a Wzrost Gospodarczy" 2017, no. 4.

Wrzosek M., Markiewicz S., Modrzejewski Z., *Informacyjny wymiar wojny hybrydowej*, Warszawa 2019.

Żebrowski A., *Agentura wpływu uczestnikiem walki informacyjnej*, „Studia nad Autorytaryzmem i Totalitaryzmem" 2018, no. 1.

Rosyjskie operacje wpływu społecznego w kontekście prowadzonej wojny kognitywnej w Ukrainie w 2022 roku

Streszczenie

W niniejszym artykule została podjęta próba zidentyfikowania rosyjskich operacji wpływu społecznego w kontekście operacji informacyjnych prowadzonych przez Federację Rosyjską podczas wojny w Ukrainie w 2022 roku. Podjęcie analizy tworzenia i rozprzestrzeniania się zagrożeń informacyjnych w wyniku podejmowanych działań przez Rosję w trwającym konflikcie jest podyktowane coraz większym wpływem procesów komunikacyjnych na globalne bezpieczeństwo. W niniejszym artykule został zaprezentowany wpływ mediów masowych na kształtowanie świadomości przez odsłonięcie mechanizmów kreowania opinii publicznej.

Słowa kluczowe: walka informacyjna, media, operacje informacyjne, dezinformacja

Krzysztof Kaczmarek*

Finland in the light of cyber threats in the context of Russia's aggression against Ukraine

Abstract

Russia's attack on Ukraine on 24 February 2022 caused Finland to put an end to its long-standing policy of finlandization and to make a decision to join the North Atlantic Treaty Organisation. Intensified Russian-inspired cyber-attacks against Finland were expected. However, over the first three quarters of 2022, no major cyber incidents occurred. In this article, the Author will undertake an attempt to answer the question as to how Finland and Finnish society defend themselves against cyber threats and whether the lack of any recorded attacks from Russia is the result of Finland's level of cyber security or the Kremlin's lack of interest in such activities.

Key words: Finland, Russia, Ukraine, NATO, security policy, cyber attack

* Krzysztof Kaczmarek, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

Introduction

Finland's application for membership in the North Atlantic Treaty Organisation (NATO) has increased the level of a threat of cyber attacks from Russia. As early as at the beginning of March 2022, Finnish services reported possible attempts by the Kremlin to interfere with Finnish public opinion. The warnings included the possibility to use both traditional and new methods, such as deep fake video[1].

In Finland, approximately 1.5 million firearms are legally in private hands. The vast majority of these include hunting weapons, but their widespread possession is also seen as a factor that increases the country's defence capability[2].

The decision to join NATO explicitly demonstrated that there was an end to many decades of the finlandization policy. After Russia's attack on Ukraine, Finland's geopolitical position changed, and an all-encompassing security strategy, based on a highly digitalised society, revealed its weaknesses. Since so many Finns possess weapons, and the country is highly digitalised, there is unfortunately a fairly high risk that Russia may already have a list of Finns with gun permits or hunting licences[3].

According to Supo (the Finnish police service responsible for the state's internal security), the worst threats to Finland's national security at the moment include Russia's extensive influence and an illegal accumulation of intelligence data. Cyber threats hit the headlines with the Russian war of aggression in Ukraine, and public interest in cyber security increased even more after Finland decided to apply for NATO membership[4].

At the same time, Finland has been preparing for cyber threats for many years by running regular drills involving both public and private entities. Their purpose is to strengthen liaison between companies and authorities in the

1 D. Mac Dougall, *Deep fakes and blackmail: Finland warns Russia could meddle in NATO membership debate*, https://www.euronews.com/2022/03/30/deep-fakes-and-blackmail-finland-concerned-about-russian-interference-in-nato-debate [access: 18.09.2022].

2 *Aseiden määrä Suomessa vähenee – katso, missä ovat maan 1,5 miljoonaa asetta*, https://yle.fi/uutiset/3-8588611 [access: 20.09.2022].

3 S. Czubowska, *Finlandia preppersem Europy. W cyberprzestrzeni zbroi się przed Rosją*, https://spidersweb.pl/plus/2022/06/finlandia-rosja-nato [access: 18.09.2022].

4 S. Hotakaisen, *Älä mene verkossa lankaan – todennäköisesti suuri perintö on huijaus*, https://www.keskipohjanmaa.fi/uutinen/640404 [access: 20.09.2022].

event of large-scale cyber incidents[5]. It would therefore appear that Finland, in terms of cyber threats, is a country of preppers. It is therefore worth examining some elements of the country's preparedness for digital threats.

Global trends in the use of digital tools against states

Harmful activities in cyberspace may take place in three ways: 1) intelligence (espionage); 2) attacks; 3) data manipulation (processing)[6]. Cyber espionage is similar to traditional intelligence and espionage activities, which aim to collect information. Data stolen and collected through cyber-intelligence may be kept secret or made public to influence public opinion and governments in a hybrid impact[7].

Two well-known hacker groups (APT 28/Fancy Bear and APT 29/Cozy Bear) linked to Russian intelligence services are known to have carried out espionage operations on computer networks against other countries. In 2015, APT 29 infiltrated the US White House information network and, in addition, the networks of several organisations in Western Europe, Central and East Asia as well as Central and South America. APT 28 was also found to have hacked into the networks of military and defence companies in the Americas, Europe and Asia. It was also behind hacks into the networks of the German Reichstag and France's TV5 Monde in 2015. Covert data collection is nothing new, but the cyber dimension brings new tools and lower costs. Cyber operations are inexpensive, the risks are low and they may produce good results. This makes cyber tools attractive for poorer countries, as well. A cyber-attack is a continuum of cyber-intelligence and it refers to an attack that targets the cyber infrastructure of the electricity, communications, water, financial and critical systems of society. To date, there have been relatively few such attacks, but this activity has increased significantly in recent years[8].

5 *Suomessa alkaa jättimäinen viranomaisten kybersotapeli, jonka käsikirjoituksesta ei hiiskuta julkisuuteen – Mukana 120 organisaatiota*, https://yle.fi/uutiset/3-12629560 [access: 20.09.2022].

6 J. Kurek, *Challenges for State Security in the Context of Big Data Analysis* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 62.

7 *Kyberuhat ja Tietoverkkovaikuttaminen*, https://turpopankki.fi/uusia-turvallisuushaasteita/hybridi-ja-kybervaikuttaminen/kyberuhat-ja-tietoverkkovaikuttaminen/#toggle-id-2 [access: 18.09.2022].

8 Ibidem.

The discovery of the Stuxnet virus in 2010 on Iranian computer systems marked the realisation of a new kind of a cyber warfare method. This „world's first digital weapon" differed from previous spyware in that, in addition to stealing data, it destroyed physical devices controlled by computers. There were two different versions of the attack: the first one damaged the centrifuges of Iran's uranium enrichment facilities and the second one manipulated the companies' computer systems. The companies in question supplied industrial control and processing systems for Iran's nuclear programme[9].

One of the most worrying attacks included a successful attack on the computer network of Telvent (a Canadian company) by the 61398 Unit (APT 1/Comment Crew/Comment Panda). The company designs remote access software for valves, switches and security systems for oil and gas companies and power grid operators. Telvent maintains detailed plans for more than a half of all oil and gas pipelines in North and South America and it has access to their systems. Cyber attacks on critical infrastructure, especially energy grids, have occurred in the context of almost all of the recent political and military crises, among others. In 2007 in Estonia, in 2008 in the Balkans and in Georgia, in Ukraine since 2014, in Syria and elsewhere in the Middle East[10].

In cyber manipulation, groups of hackers may manipulate or alter data stored on a computer network once it has entered the system. Manipulation could be a major challenge in the future. To date, most intrusions into computer networks include data theft. The threat is that an intruder will begin to manipulate and alter data so that the network owner may no longer believe and trust their own system. James Clapper, the former US Director of National Intelligence (DNI), expressed his concern by saying, „I believe we will see more cyber operations that alter or manipulate electronic information to compromise its integrity". One of the most serious incidents of electronic manipulation occurred in 2013, when Syrian hackers accessed the Twitter account of the Associated Press news agency and tweeted fake news about an explosion at the White House. This also had a direct impact on interest rates on the US stock market. One of the first attempts to manipulate data to achieve political ends occurred during the 2016 US presidential election. Russian hackers who gained access to the Illinois voter database attempted to alter the electoral roll data, yet without any success[11].

9 Ibidem.
10 Ibidem.
11 Ibidem,

In 2017, there occurred a lot of ransomware (ransomware; WannaCry, NotPetya and BadRabbit) in an almost epidemic fashion. In 2018, it was revealed how inadequate the capabilities are to face cyber threats related to side-channel attacks and vulnerabilities in microprocessors as well as in various components and devices (infringed components). In the year 2019, covert military operations related to interstate conflicts started to take place in cyberspace. For this reason, cyber threat researchers around the world have begun to shift their focus from financially motivated cyber criminals to state-sponsored cyber operations. In the recent years, the Internet of Things has introduced a new dimension to the cyber world that can be used in cyber operations. Due to the low level of security of devices, it is possible to access computer networks and spread malware through these[12].

Governments' activities in cyberspace

The cyber activities on the part of governments and the groups they support are primarily focused on intelligence. There are more than a hundred active groups worldwide, which have been linked to organisations in almost 20 countries. These organisations include South Korea, India, Iran, Israel, Lebanon, Nigeria, Pakistan, Palestine, North Korea, Syria, Russia, Vietnam, Turkey, the United Arab Emirates and the United States, among others. Several Western countries, such as the UK, France, Germany and the United States, operate in cyberspace with actors involved in intelligence and defence organisations[13].

Cyber operations, in combination with other means of hybrid influence, have created opportunities for governments to act in ways that can be carried out, at least to some extent, in secret and in such a way that states' involvement in matters that come to light can be denied. Offensive cyber operations were used in particular in the context of the crisis in Ukraine and the occupation of Crimea, as well as in the Middle East in the context of the Syrian civil war and the situation in Iran[14].

From among government-sponsored cyber operators, Russian actors are the most active ones and have caused the worst damage. Since 2014, their main

12 Ibidem.
13 Ibidem.
14 Ibidem.

target has been the Ukrainian government and its law enforcement and armed forces. Since 2017, Russian actions have also targeted critical infrastructure and the energy sector in Europe and the United States, such as nuclear power plants. At least seven Russian groups, operating under different names, have been identified[15].

Chinese groups have been observed to be oriented towards the requirements set out in the government's Made in China 2025 plan for the technology, energy and healthcare sectors. There has been an increase in the activities of the Chinese groups in recent years, which is at least partly related to the deterioration of the US-China relations[16].

In recent years, Iranian groups have intensified their operations owing to new tactics, techniques and procedures. These include, for example, strategic hacking campaigns and mobile malware. These have been used against regional rivals to constrain the opposition's activities at home, as well as to support their own „soft war" campaigns. North Korean groups have also increased their activity recently. Their areas of interest include mainly the financial sector and intelligence targeting South Korea[17].

Expert recommendations to Finnish society in the event of a large-scale cyber incident

Cyber threats are not bound by place, time or national borders, and improper conduct or damage does not always meet the criteria of a crime under existing national laws. This is particularly true for disinformation activities. Since the Russian invasion of Ukraine, the European Union has imposed a series of harsh sanctions on Russia, and some Kremlin-controlled news services have lost their ability to broadcast in the territory of the Community. However, Russian-language search results on Apple and Google still mainly include news sources spreading Kremlin propaganda[18].

15 Ibidem.
16 Ibidem.
17 Ibidem.
18 J. Kullas, *Noudattavatko teknologiajätit Venäjä-pakotteita? Applen Siri mainostaa Kremlin propagandaa*, https://www.mikrobitti.fi/uutiset/noudattavatko-teknologiajatit-venaja-pakotteita-applen-siri-mainostaa-kremlin-propagandaa/5c661f7c-2863-4863-aea5-12261a2707eb [access: 18.09.2022].

Based on historical experience, Finnish society has long been preparing for crisis situations. At the same time, procedures for dealing with emergency situations are being developed on an ongoing basis. Following Russia's attack on Ukraine and Finland's declaration to join NATO, Finnish-Russian relations have cooled considerably.

According to Finland's Traficom National Cyber Security Centre, the number of cyber threats to Finland will increase as the country joins the North Atlantic Treaty Organisation[19].

One of the signals of an incipient Russian cyber-attack on Finland is likely to be a disinformation campaign referring to history and portraying past events in a light intended to cause social division and to discredit Western countries in the eyes of Finnish society. Similar incidents took place in Estonia in 2007. There was civil unrest at the time and the country was subjected to numerous cyber attacks. At the same time, immediately prior to the military attack, Russia inspired a number of cyber attacks on Ukraine[20].

The Finnish authorities are preparing the public for cyber attacks on the assumption that the most effective disruption to the normal functioning of the state may be caused by the technically simplest „denial of service" attacks, which cause online services to fail. Immediately prior to the attack, Russia had attacked Ukraine's financial, telecommunications, software, energy and healthcare sectors in this way. In addition, water supply, trade and distribution sectors were attacked, including the media sector[21].

Regardless of the global geopolitical situation, an increase in the number of attempted cyber attacks on Finland has been observed since the beginning of 2019, but these have not been successful. In spring 2022, however, there were a few rare „denial of service" attacks on government websites in Finland. A „denial of service" attack puts so much strain on a company or organisation's public website that its network crashes. In addition, GPS signal jamming was observed in Finland during that same period[22].

It seems that most of Finnish society are prepared to reduce the impact of cyber attacks by following several basic principles. Finnish experts indicate that society will be prepared for cyber attacks provided that every citizen is

19 *Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin – listaamme kuusi tapaa*, https://yle.fi/uutiset/3-12440524 [access: 21.09.2022].
20 Ibidem.
21 Ibidem.
22 Ibidem.

prepared. To this end, they recommend first and foremost that every household should have enough provisions to function for at least a few days without any additional supplies[23].

They also point out that any type of an attack on the banking sector may result in an inability to use services that require bank identification to log in, such as the police or health care system. The impact of such attacks can be reduced by using the services of two different banks. One should also perform activities that require bank identification well in advance of the deadline. Mobile verification can also be used, but again, it is safer to have two SIM cards from different operators[24].

In the majority of cases, Finns follow the recommendations on what steps to take when electronic payment systems (including cards) are not working by possessing enough cash for expenses necessary for a period of a few days. However, the recommendations are to have both payment cards from two different banks and cash[25].

According to experts, considering the level of preparedness on the part of energy companies, a denial-of-service attack is unlikely to cause power outages in Finland. However, even this is not completely out of question. Therefore, they recommend having an emergency power source, e.g. a power bank. It is also recommended to have a battery-powered radio, as it may be the only source of information in the event of a crisis. In addition to technical aspects, it is also disinformation campaigns that may have serious consequences. Finns are alert to this possibility especially in the context of Russia's aggressive policy. The Finnish authorities are sensitising Finnish society particularly to information related to refugees[26].

Countering cyber attacks and their impact in Finland

The most common cyber threats in Finland include ransomware, denial of service attacks and data leaks. Attacks on IT service providers have also become more common. More lasting damage is caused by the destruction of IT systems and data repositories, which also aims to increase uncertainty

23 Ibidem.
24 Ibidem.
25 Ibidem.
26 Ibidem.

in conflict situations. In order to be prepared for cyber threats, institutions must be able to identify the targets to be protected and determine which of these are the most important ones. What does an organisation need to do to guarantee basic security? Who ultimately has access to strategic data and has the security of the cloud services used by the organisation been thought through to the end? Ensuring cyber security requires answers to these questions. Remote working brings with it new risks associated with a transition from a company-controlled network to unattended networks. In addition, the use of employees' own devices exposes them to security risks[27].

Technical protection provides a solid foundation for cyber security. Criminals often look for easy targets with vulnerabilities. A good firewall is the minimum level at which an institution demonstrates that it is prepared for cyber threats[28]. Good technical security is created by automatic software updates, identified users as well as strong and different passwords for different services. In an increasingly mobile world, it is worth remembering that mobile tools are also vulnerable to security incidents.

Security of administrative information also constitutes one element of being prepared for cyber threats. Good governance and risk management enable smooth operations and minimise potential threats. Research confirms that in Finland, institutions are well prepared for cyber threats, with trainings focused on the knowledge of procedures and their actual implementation in the case of threats.

Conclusions

Russia's attack on Ukraine on 24 Feb. 2022 changed the geopolitical shape of the world. The balance of security also changed. Finland's position on the international stage also changed. Situated on the geographical periphery of Europe, the country has always sought to balance relations between the blocs formed by the superpowers. However, in terms of preventing cyber threats, Finland's line of conduct has not changed. The country's authorities and its

27 M. Långström, *Mitä organisaatiot voivat tehdä varautuakseen kyberuhkiin*?, https://www.rakli.fi/rakli-tiedottaa/mita-organisaatiot-voivat-tehda-varautuakseen-kyberuhkiin/ [access: 21.09.2022].

28 W. Pizło, *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension*..., p. 141.

society seem to be prepared for most attacks taking place in cyberspace. This is most certainly due to the historical experience of Finland, which has been exposed to threats from its eastern neighbour for centuries and, in particular, in the 20th century. Both Finland's domestic, foreign and security policies are multifaceted and are constantly evolving, and in the era of cyber society, cyber security has become an integral part of national security[29]. Apart from some spectacular attacks, such as the suspension of the Parliament's website, there is no widely known information concerning serious cyber-attacks on Finland. There seem to be three possible explanations for this: 1) Finland is perfectly prepared and repels all attacks; 2) successful attacks are concealed; 3) the possibilities of Russia's hostile cyber activities are overestimated.

Obviously enough, Russia should not be underestimated, yet being aware of threats makes it possible to counter them and minimise any potential losses in the event of a successful cyber attack. Therefore, Finland appears to be a country that is well prepared for cyber threats.

Bibliography

Aseiden määrä Suomessa vähenee – katso, missä ovat maan 1,5 miljoonaa asetta, https://yle.fi/uutiset/3-8588611 [access: 20.09.2022].

Czubowska S., *Finlandia preppersem Europy. W cyberprzestrzeni zbroi się przed Rosją*, https://spidersweb.pl/plus/2022/06/finlandia-rosja-nato [access: 18.09.2022].

Hotakaisen S., *Älä mene verkossa lankaan – todennäköisesti suuri perintö on huijaus*, https://www.keskipohjanmaa.fi/uutinen/640404 [access: 20.09.2022].

Kullas J., *Noudattavatko teknologiajätit Venäjä-pakotteita? Applen Siri mainostaa Kremlin propagandaa*, https://www.mikrobitti.fi/uutiset/noudattavatko-teknologiajatit-venaja-pakotteita-applen-siri-mainostaa-kremlin-propagandaa/5c661f7c-2863-4863-aea5-12261a2707eb [access: 18.09.2022].

Kurek J., *Challenges for State Security in the Context of Big Data Analysis* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Långström M., *Mitä organisaatiot voivat tehdä varautuakseen kyberuhkiin*?, https://www.rakli.fi/rakli-tiedottaa/mita-organisaatiot-voivat-tehda-varautuakseen-kyberuhkiin/ [access: 21.09.2022].

Mac Dougall D., *Deep fakes and blackmail: Finland warns Russia could meddle in NATO membership debate*, https://www.euronews.com/2022/03/30/deep-fakes-and-blackmail-finland-concerned-about-russian-interference-in-nato-debate [access: 18.09.2022].

Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin – listaamme kuusi tapaa, https://yle.fi/uutiset/3-12440524 [access: 21.09.2022].

Pizło W., *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

29 D. Tyrawa, *The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity* [in:] *The Public Dimension*..., p. 23.

Suomessa alkaa jättimäinen viranomaisten kybersotapeli, jonka käsikirjoituksesta ei hiiskuta julkisuuteen – Mukana 120 organisaatiota, https://yle.fi/uutiset/3-12629560 [access: 20.09.2022].
Tyrawa D., *The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Finlandia wobec cyberzagrożeń w kontekście agresji Rosji na Ukrainę

Streszczenie

Atak Rosji na Ukrainę 24 lutego 2022 roku spowodował, że Finlandia skończyła z długoletnią polityką finlandyzacji i zdecydowała się na przystąpienie do Paktu Północnoatlantyckiego. Spodziewano się skierowanych przeciwko niej zintensyfikowanych ataków cybernetycznych inspirowanych z Rosji. Jednakże przez pierwsze trzy kwartały 2022 roku nie doszło do żadnych poważnych incydentów cybernetycznych. W artykule autor podjął próbę odpowiedzi na pytania: w jaki sposób Finlandia i społeczeństwo tego państwa bronią się przed cyberzagrożeniami oraz czy brak odnotowanych ataków ze strony Rosji jest skutkiem poziomu cyberbezpieczeństwa Finlandii czy też braku zainteresowania Kremla takimi działaniami.

Słowa kluczowe: Finlandia, Rosja, Ukraina, NATO, polityka bezpieczeństwa, cyberatak

Sławomir Stalmach*

Polskie media o wojnie w Ukrainie – przegląd ważniejszych wydarzeń pierwszego półrocza 2022 roku

Streszczenie

Wojna, którą prowadzi Rosja przeciwko Ukrainie od 24 lutego 2022 roku, jest brutalna i określana jako pełnoskalowa, tj. z wykorzystaniem wszystkich sił i środków. W erze dynamicznie rozwijających się mediów także informacja stała się bronią, która jest świadomie używana w tym konflikcie.

Dokonując przeglądu najważniejszych informacji, które znalazły się w centrum zainteresowania dużej części mediów w Polsce podczas pierwszego półrocza od napaści Rosji na Ukrainę, można stwierdzić, że obszernie informują one o wojnie w Ukrainie, ale nie ograniczają się jedynie do relacjonowania konfliktu, odnoszą się także do dezinformacji i propagandy, a nawet dotykają sfery resentymentów, które są wciąż żywe pomiędzy różnymi krajami. Zestawienie informacji uzmysławia jak ważną rolę we współczesnym świecie odgrywają media oraz że dbałość o ich rozwój i zabezpieczenie infrastruktury medialnej jest strategicznym zadaniem państwa.

Słowa kluczowe: media, wojna w Ukrainie, cyberbezpieczeństwo, dezinformacja

* Sławomir Stalmach, Ośrodek Implementacji Nowoczesnej Technologii Cyberbezpieczeństwa, Akademickie Centrum Polityki Cyberbezpieczeństwa, Akademia Sztuki Wojennej, e-mail: s.stalmach@akademia.mil.pl, ORCID: https://orcid.org/0000-0001-5679-4645.

Media i dezinformacja

Nie ma jednej definicji mediów, która opisuje proces przekazywania informacji pomiędzy ludźmi[1]. Właściwie nadal musimy zadowalać się ogólną refleksją przedstawioną przez Parmenidesa i Platona[2], że myśl z jednej głowy przechodzi do drugiej za pomocą jakiegoś pośrednika (tzw. koncepcja metaxy, od starogreckiego przyimka, który oznaczał coś między czymś lub wskazywał na to, co jest pośrodku). Tym pośrednikiem są ludzie – mediatorzy lub jakieś rzeczy specjalnie do tego przeznaczone lub stworzone, np. prasa czy eter. Tak samo nie ma jednej definicji dezinformacji występującej w mediach. Dezinformacja stale towarzyszy komunikacji międzyludzkiej, ale jej obecny rozwój można łączyć z rozkwitem mediów w internecie, gdzie powstały dogodne warunki do rozprzestrzeniania się fałszywek. Głównie dlatego, że współczesne media, czyli prasa, radio i telewizja, są niemal w całości dostępne w internecie.

Wydawać by się mogło, że od momentu napaści Rosji na Ukrainę będziemy mieli do czynienia ze wzmożeniem planowanego używania dezinformacji na potrzeby wojny. Oczywiście, to nastąpiło, ale dezinformacja okazała się tylko jednym z wielu narzędzi propagandy, i nie najważniejszym. Weszła do arsenału innych środków wojennych i tym samym straciła walor czegoś wyjątkowego, jaki miała jeszcze przed wojną. Dezinformacja stała się jedynie jednym z działań w katalogu akcji wojennych. Na potrzeby wojny nie wystarczy kłamać, bo to za mało, należy budować różnorodne, pełnoskalowe działania propagandowe.

To jest jeden z wniosków, jakie wynikają z analizy istotnych z punktu widzenia mediów wydarzeń z pierwszego półrocza wojny prowadzonej przez Rosję przeciwko Ukrainie w 2022 roku.

Metodologia badań

Badanie było prowadzone z wykorzystaniem metody teorii ugruntowanej (czasami nazywanej metodą ugruntowaną lub MTU). Uważa się, że twórcami tego sposobu naukowego badania są: Barney Glaser[3], Kathy Charmaz[4],

1 D. Mersch, *Teorie mediów*, Warszawa 2010.
2 Platon, *Uczta*, Warszawa 1994, s. 96–97.
3 B. Glaser, *Getting Started*, „The Grounded Theory Review" 2020, t. 19, nr 1.
4 K. Charmaz, *Teoria ugruntowana. Praktyczny przewodnik po analizie jakościowej*, Warszawa 2009.

a także Krzysztof Konecki[5]. Naukowcy z niej korzystający analizują jakiś problem zgodnie z rozumowaniem indukcyjnym na podstawie zebranych różnorodnych danych, w tym medialnych. Dodając kolejne dane, z czasem zaczyna się wyłaniać konkretna teoria. Wreszcie, dochodzi do tzw. nasycenia, czyli momentu, w którym badacze osiągają pewność, że kolejne dane nie zmienią istotnie wysnutego wniosku.

Najważniejsze dla omawianego badania było przyjęcie definicji, czym są główne wydarzenia z punktu widzenia mediów. Dla wszystkich typów redakcji, tj. gazetowych, radiowych, telewizyjnych, internetowych, w tym tzw. mediów społecznościowych, obecnie najważniejsze są dwa wymiary – powszechność i opiniotwórczość. Powszechność to – zależnie od typu mediów – nakład, słuchalność, oglądalność, klikalność i zasięgi. Opiniotwórczość wpływa na renomę i poważanie redakcji, co przekłada się na pozycję tytułu na rynku medialnym. Dlatego ważnymi wydarzeniami z punktu widzenia mediów są nie tylko te informacje, które spotykają się z powszechnym zainteresowaniem, ale także te, które stanowią o marce danego tytułu. Każda redakcja ważne informacje oznacza w sposób szczególny, np. są one umieszczane w najważniejszym miejscu, są opatrywane wykrzyknikiem lub hasłem typu Breaking News czy edytorial, do nich stosuje się pogrubienie, dołącza obszerne omówienie itp.

W badaniu za główne wydarzenia z punktu widzenia mediów uznano te, które zarazem powszechnie rezonują, czyli rozchodzą się wiralowo, oraz te, które zostały uznane za szczególnie ważne przez poszczególne redakcje. Były zamieszczane z emfazą przez wiele redakcji równocześnie oraz natychmiast zyskiwały ogromne zainteresowanie odbiorców. Przeglądając różne media z pierwszego półrocza wojny w Ukrainie, dało się zauważyć, że niektóre informacje pojawiały się w kilku tytułach równocześnie i zajmowały zainteresowane redakcje w sposób szczególny.

Badaniu były poddanie media publikujące w języku polskim: prasa, radio, telewizja, które mają swoje strony internetowe, a także te, które wyłącznie ukazują się w internecie.

Przyjęto, że badanie będzie obejmowało 6 miesięcy od dnia napaści Rosji na Ukrainę, tj. od 24 lutego do 24 sierpnia 2022 roku. Jednakże wojna w Ukrainie nie wybuchła z dnia na dzień, dlatego zdecydowano się na analizę także

5 K. Konecki, *Wizualna teoria ugruntowana. Podstawowe zasady i procedury*, „Przegląd Socjologii Jakościowej" 2012, t. 7, nr 1.

wybranych zdarzeń z kilku miesięcy poprzedzających inwazję wojsk rosyjskich na terytorium Ukrainy.

Główne wydarzenia, z punktu widzenia mediów, charakteryzują się tym, że występują w różnych mediach jednocześnie, dlatego do wskazania poszczególnych zdarzeń wystarczy przywołanie jednej spośród wielu redakcji. Wszystkie obrazy użyte w prezentacji są screenami otwartych stron internetowych i są wykorzystywane jedynie w celu ilustracji analizy naukowej.

Badanie wymagało w pierwszej kolejności zestawienia kalendarium głównych wydarzeń z punktu widzenia mediów, warto bowiem zobaczyć jak wiele informacji następowało jedna po drugiej i jak szybko kolejne zdarzenia wypierały poprzednie. Następnie podjęto próbę wyciągnięcia analitycznych wniosków z tak zestawionego diariusza. Najważniejsze wnioski dotyczą po pierwsze, konieczności zadbania przez państwo o infrastrukturę medialną na wypadek konfliktu oraz pod drugie, potrzeby budowania świadomości społecznej, zwłaszcza, czym jest racja stanu, a czym wroga propaganda.

Kalendarium ważniejszych wydarzeń medialnych

Autor artykułu dokonał przeglądu ważniejszych faktów, dezinformacji i działań propagandowych związanych z atakiem Rosji na Ukrainę, które były powszechnie dyskutowane w polskich mediach i uznane za ważne z punktu widzenia różnych redakcji. W nawiasach podano tylko jedno, wybrane źródło danej informacji, screeny zdjęć służą jedynie ilustracji danej informacji do celów naukowych i pochodzą z różnych stron internetowych czy mediów społecznościowych.

Początek czerwca 2021 – Białoruś rozpoczęła operację specjalną skierowaną przeciwko Litwie, Łotwie i Polsce. Na Białoruś są sprowadzani rzekomi emigranci, skąd próbuje się ich przepchnąć przez granice do Polski, Litwy i Łotwy. Medialnie operację popierali tzw. pożyteczni idioci[6].

6 N. Makarewicz, A. Zygiel, M. Partyła, *Tysiące migrantów przy granicy polsko-białoruskiej. Rozbili obóz w rejonie Kuźnicy*, RMF24, 2021, https://www.rmf24.pl/raporty/raport-kryzys-na-pograniczu/news-tysiace-migrantow-przy-granicy-polsko-bialoruskiej-rozbili-o,nId,5632401#crp_state=1 [dostęp: 5.01.2023].

Źródło: https://www.rmf24.pl/raporty/raport-kryzys-na-pograniczu/news-tysiace-migrantow-przy-granicy-polsko-bialoruskiej-rozbili-o,nId,5632401#crp_state=1 [dostęp: 5.01.2023].

Fot. 1. Próba sforsowania granicy białorusko-polskiej

Przełom 2021 i 2022 – Rosja zgromadziła ponad 100 tys. żołnierzy przy granicy z Ukrainą, a także na granicy Białorusi i Ukrainy. Pod koniec listopada 2021 roku Stany Zjednoczone udostępniły swoim europejskim sojusznikom dane wywiadowcze wskazujące na możliwość wielokierunkowego ataku Rosji na Ukrainę.

11 lutego 2022 – Amerykanie ostrzegali przed wojną i ujawnili swoje szpiegowskie analizy. Na briefingu w Białym Domu doradca ds. bezpieczeństwa narodowego Jake Sullivan mówił, że atak Rosji na Ukrainę może rozpocząć się około 20 lutego.

23 lutego – Unia Europejska przyjęła pakiet sankcji wobec Rosji w odpowiedzi na decyzję Kremla o wysłaniu wojsk do obwodów donieckiego i ługańskiego.

24 lutego 2022, godz. 3.45 – rosyjska telewizja wyemitowała wystąpienie prezydenta Rosji Władimira Putina, który ogłosił, że Rosja rozpoczyna „specjalną operację militarną" w obronie samozwańczych republik na wschodzie

Ukrainy, kilka dni wcześniej uznanych przez Rosję za niepodległe państwa. Putin zapowiedział, że celem Rosji nie jest „okupacja Ukrainy", ale siły rosyjskie będą dążyły do „demilitaryzacji Ukrainy" i jej „denazyfikacji". Putin dodał, że Rosja nie pozwoli Ukrainie „wejść w posiadanie broni nuklearnej"[7].

Źródło: https://natemat.pl/398711,putin-wypowiedzial-wojne-przemowienie-prezydenta-rosji [dostęp: 5.01.2023].

Fot. 2. Telewizyjne wystąpienie Władimira Putina

24 lutego – nie działała żadna informacyjna telewizja ukraińska. Ukraińcy dowiedzieli się o wojnie głównie z telewizji rosyjskich i amerykańskich. Największa stacja informacyjna Ukraina24 w nocy z 23 na 24 lutego nie pracowała.

24 lutego cały dzień – wszystkie media na całym świecie pokazywały obrazy z napadniętej Ukrainy, głównie exodus Ukraińców i przemówienia prezydenta Wołodymyra Zełeńskiego oraz nieliczne ujęcia z przekraczania granicy przez wojska rosyjskie i pierwsze zdjęcia ostrzelanych rakietowo budynków mieszkalnych[8].

7 T. Ławnicki, *Tak Putin wypowiedział wojnę. Okoliczności wymagają od nas natychmiastowych działań*, NaTemat, 2022, https://natemat.pl/398711,putin-wypowiedzial-wojne-przemowienie-prezydenta-rosji [dostęp: 5.01.2023].

8 H. Ossowski, *Sznur aut na wyjeździe z Kijowa. Mieszkańcy uciekają ze stolicy Ukrainy*, Wirtualna Polska, 2022, https://wiadomosci.wp.pl/sznur-aut-na-wyjezdzie-z-kijowa-ludzie-uciekaja-ze-stolicy-ukrainy-6740734577269664a [dostęp: 5.01.2023].

Źródło: https://wiadomosci.wp.pl/sznur-aut-na-wyjezdzie-z-kijowa-ludzie-uciekaja-ze-stolicy-ukrainy-6740734577269664a [dostęp: 5.01.2023].

Fot. 3. Sznur aut na drogach wyjazdowych z Kijowa

Źródło: https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-zaciete-walki-w-kijowe-rosyjski-pocisk-trafil-w-blok-mieszka,nId,5857126#crp_state=1 [dostęp: 5.012023].

Fot. 4. Zniszczony budynek mieszkalny w Kijowie

24 lutego wieczorem – prezydent Stanów Zjednoczonych Joe Biden ogłosił sankcje, które „będą słono kosztować rosyjską gospodarkę zarówno w krótkim, jak i w długim okresie".

Od 24 lutego przez cały czas – media informowały o wszechstronnej pomocy udzielanej przez Polaków sąsiadom z Ukrainy.

25 lutego – świat obiegł wiralowo film internetowy, w którym obrońcy Wyspy Węży mówią: „Russkij wojennyj korabl, idi na chuj!" Była to odpowiedź Ukraińców na dictum dowódcy rosyjskiego statku wojennego, który zaatakował placówkę ukraińską na tej wyspie. Wszyscy obrońcy mieli zginąć tuż po tych słowach w wyniku ostrzału rosyjskiego. Później okazało się, że nikt nie zginął, a obrońcy zostali wzięci do niewoli, z której po 3 miesiącach zostali zwolnieni. Sformułowanie stało się zawołaniem bojowym ukraińskich żołnierzy[9].

Źródło: https://www.wprost.pl/wojna-na-ukrainie/10636126/bohaterska-smierc-obroncow-wyspy-wezy-rosyjski-okrecie-wojenny-spielaj.html [dostęp: 5.01.2023].

Fot. 5. Rosyjski okręt wojenny widziany z Wyspy Węży

26 lutego – rząd Niemiec ogłosił decyzję o wysłaniu broni do Ukrainy, potwierdził to dzień później podczas przemówienia w Bundestagu kanclerz Olaf Scholz. W praktyce, Niemcy ociągały się z wysyłaniem obiecanej broni.

9 *Bohaterska śmierć obrońców Wyspy Węży. Rosyjski okręcie wojenny, spie***laj*, Wprost.pl, 2022 https://www.wprost.pl/wojna-na-ukrainie/10636126/bohaterska-smierc-obroncow-wyspy-wezy-rosyjski-okrecie-wojenny-spielaj.html [dostęp: 5.01.2023].

28 lutego – ukazał się kontrowersyjny wywiad z ambasadorem Rosji w Polsce, udzielony tygodnikowi „Sieci". Pismo było krytykowane za udostępnienie swoich łam do szerzenia propagandy rosyjskiej[10].

ATAK ROSJI NA UKRAINĘ

Rosjo, dlaczego to robisz?

Kiedy dotarła do nas – złożona przez pośrednika – propozycja przeprowadzenia wywiadu z ambasadorem Rosji w Polsce, zawahaliśmy się. Zarzuty, które padną przy tej okazji, są oczywiste i łatwe do przewidzenia. Uznaliśmy jednak, że warto nawet w tak napiętej sytuacji zapytać twardo i bezkompromisowo o te kwestie, które są dla polskiej opinii publicznej ważne. Rozmowa odbyła się we wtorek 22 lutego, kiedy wydawało się, iż rosyjskie działanie – choć też bezprawne – ograniczy się do terenu zajmowanego przez tzw. republiki ługańską i doniecką. Dwa dni później rozpoczął się pełnoskalowy atak Rosji na Ukrainę. Znowu stanęliśmy przed dylematem. Uznaliśmy jednak, że zapis tej rozmowy jest ważnym dokumentem, pozwala Polakom lepiej wejrzeć w rosyjski sposób myślenia i działania, przedstawiony przez dyplomatę wysokiej rangi, i zastanowić się, w jaki sposób odpowiedzieć na stojące przed nami wyzwania. A są to wyzwania zarówno militarne, wynikające z nieskrywanych już ambicji nuklearnych, jak i dotyczące np. postępującej instrumentalizacji historii. Dlatego zdecydowaliśmy się wydrukować (autoryzowany przez ambasadora) zapis tej rozmowy, pomimo że Rosja zaatakowała sąsiednie państwo zbrojnie, a więc dokonała rzeczy w istocie wykluczającej ją ze wspólnoty państw cywilizowanych. Zdajemy też sobie sprawę, że wiele podawanych przez naszego rozmówcę faktów mija się z prawdą, a sporo jego ocen wymaga riposty. Staraliśmy się reagować już w trakcie rozmowy, choć wtedy było to możliwe, co zrozumiałe, tylko w ograniczonym zakresie

Jacek i Michał Karnowscy rozmawiają z ***Siergiejem Andriejewem****, ambasadorem Federacji Rosyjskiej w Warszawie*

Zdjęcia Andrzej Stawarczyński

Panie ambasadorze, trudno nam zrozumieć, dlaczego Rosja podobno bratniemu narodowi ukraińskiemu robi takie rzeczy? Wojsko na granicach, zastraszanie, wręcz terroryzowanie. Dlaczego Rosja robi to Ukraińcom?

Siergiej Andriejew: Ukraińcy to nie tylko naród bratni, prezydent Putin wielokrotnie mówił, że faktycznie jesteśmy tym samym narodem. Chodzi nie o naród, ale o władze, o reżim, z którym rzeczywiście mamy problemy, bo ci ludzie robią z Ukrainy tzw. anty-Rosję. Przyjęli nastawienie antyrosyjskie, prowadzą działania antyrosyjskie, które stały się sensem istnienia tego reżimu. Wykorzystują ten ukraiński reżim obce mocarstwa, Ukraina staje się bazą do prowadzenia działań przeciw mojemu krajowi.

wPolityce.pl

Jak możemy tego nie widzieć? Nie wyciągać z tych faktów konsekwencji?

Mówi pan o „reżimie". Ale już po Majdanie w 2014 r. były jedne wybory prezydenckie, które wygrał prezydent Poroszenko, potem kolejne, które przegrał i prezydentem został Zełenski. Odbywają się też demokratyczne wybory parlamentarne, jest pluralistyczna scena medialna, szanowane są prawa człowieka. Słowo „reżim" użyte w tym kontekście jest odwróceniem jego sensu. To Rosja jest raczej państwem silnie scentralizowanym z – powiedł pan ambasador na naszą opinię – w dużej mierze fikcyjną sceną polityczną.

Formalnie uznajemy, że władza ukraińska jest wykłonna w trakcie wyborów konstytucyjnych, legitymizowana w wyborach. Problem jest w tym, że naszym zdaniem nie reprezentuje ona rzeczywistych interesów i woli narodu ukraińskiego. Zarówno Poroszenko, jak i Zełenski szli do wyborów pod hasłami pokoju, uregulowania kryzysu na wschodzie kraju, polepszenia stosunków z Rosją, a po dojściu do władzy robią coś zupełnie odwrotnego.

Co do rosyjskiego systemu politycznego – kształtujemy go zgodnie z warunkami i potrzebami naszego kraju, przywiązując zasadniczą wagę do zapewnienia stabilności, rozwoju i bezpieczeństwa. To odpowiada interesom przytłaczającej większości obywateli rosyjskich, co znajduje odzwierciedlenie podczas regularnych, całkiem demokratycznych i bynajmniej nie fikcyjnych wyborów. Na tle tego politycznego burdelu, który nie kończy się przez wiele lat na Ukrainie, skuteczność naszego systemu politycznego wydaje się tym bardziej oczywista.

Czy naprawdę można mówić o jakimkolwiek zagrożeniu? Naszym zdaniem nie i cała ta nagonka jest po prostu wielką operacją dezinformacyjną. Mówi się stale o zagrożeniu wielką operacją rosyjską, snuje scenariusze zajęcia Kijowa, zajęcia całego kraju

Nawet gdyby na Ukrainie tak było, jak pan mówi, to jest to cecha demokracji, wewnętrzne prawo poszczególnych państw do definiowania własnych interesów, nawet do zmiany linii politycznej. Gdyby z tego czynić warunek uzasadniający działania zbrojne, to na świecie kamień na kamieniu by nie został.

Cóż, tylko wyjaśnijmy panom, dlaczego uważamy, iż ta władza nie reprezentuje narodu ukraińskiego, nie odpowiada jego rzeczywistym interesom.

Prezydent Putin idzie dalej: mówił w swoim głównym wystąpieniu w ubiegłym tygodniu, że Ukraina nigdy nie była prawdziwym narodem, że jest nieodłączną częścią Rosji. To jest, panie ambasadorze, i upoważnione Ukrainiec, i nieprawda. O tożsamości narodowej decyduje wola społeczna, język, historia.

Ale tutaj tę tożsamość narodową sztucznie buduje się na negowaniu autentycznej historii Ukrainy, na sztucznym przeciwstawianiu się Rosji, budowaniu anty-Rosji. To jest fundamentem istnienia reżimu w Kijowie i to nie ma racjonalnych podstaw. Tego uznać nie możemy.

Jakiej zatem Ukrainy Rosja by chciała? Jakiej dałaby spokój?

Źródło: https://wpolityce.pl/polityka/587569-tak-opublikowalismy-zapis-rosyjskiej-psychy-i-klamstwa [dostęp: 5.01.2023].

Fot. 6. Artykuł opublikowany w tygodniku „Sieci"

28 lutego – BBC usunęła ze swojego portalu kłamliwy tweet uderzający w Polskę. Opisywał on rzekome szykany z powodu koloru skóry, jakich miał doznać nigeryjski student Gabriel, który przekraczał granicę ukraińsko-polską. Wycofanie tweetu zostało uznane za sukces działań w stylu: presja ma sens[11].

10 M. Karnowski, *Tak, opublikowaliśmy zapis rosyjskiej psychy i rosyjskiego kłamstwa. I od razu tak to nazwaliśmy. To ważny dokument, Polacy muszą to wiedzieć*, wPolityce, 2022, https://wpolityce.pl/polityka/587569-tak-opublikowalismy-zapis-rosyjskiej-psychy-i-klamstwa [dostęp: 5.01.2023].

11 *Presja ma sens. BBC usunęła kłamliwy tweet uderzający w Polskę*, Tysol.pl, 2022, https://www.tysol.pl/a79856-presja-ma-sens-bbc-usunela-klamliwy-tweet-uderzajacy-w-polske [dostęp: 5.01.2023].

Źródło: https://www.tysol.pl/a79856-presja-ma-sens-bbc-usunela-klamliwy-tweet-uderzajacy-w-polske [dostęp: 5.01.2023].

Fot. 7. Student Gabriel z reportażu BBC

2 marca – operator gazociągu Nord Stream 2 zamknął działalność.

3 marca – w „Le Figaro" został opublikowany kłamliwy artykuł o tym, że Polska jest zaledwie pośrednikiem dla innych państw w sprawie pomocy dla Ukrainy.

4 marca – wiralowo rozprzestrzeniał się fake news o tym, że aktor Leonardo DiCaprio przekazał 10 mln dolarów wsparcia dla Ukrainy.

5 marca – ukraińska piosenka pod tytułem „Bayraktar" stała się światowym hitem w internecie.

8 marca – pokerowe zagranie polskiego MSZ w sprawie przekazania samolotów do Ukrainy. Polskie MSZ zadeklarowało, że Polska jest gotowa przemieścić wszystkie swoje samoloty MiG-29 do bazy w Ramstein i oddać do dyspozycji NATO, żeby zostały przekazane do Ukrainy. Ucięło to dyskusję na temat, czy przekazywać samoloty do Ukrainy i kto ma to zrobić – dowództwo NATO czy poszczególne kraje[12]?

12 *Oświadczenie Ministra Spraw Zagranicznych Rzeczypospolitej Polskiej w związku z wypowiedzią Sekretarza Stanu USA w sprawie przekazania samolotów Ukrainie*, MSZ, Warszawa, 2022, https://

9 marca – w internecie został pokazany spreparowany film o płaczącym malcu na granicy w Medyce, którym nikt się nie zajął. Straż Graniczna zdementowała tego fake newsa – przy chłopczyku byli rodzice, ale na filmie ich nie pokazano[13].

Źródło: https://rzeszow.wyborcza.pl/rzeszow/7,34962,28199741,fake-news-malec-ktory-mial-sam-przekroczyc-granice-w-medyce.html [dostęp: 5.01.2023].

Fot. 8. Płaczący chłopczyk na granicy w Medyce

11 marca – prezydent Ukrainy Wołodymyr Zełenski przemawiał z wykorzystaniem łączy internetowych przed polskim parlamentem. Później także przed parlamentami: Niemiec, Francji, Finlandii, Słowacji, Czech, Łotwy, Japonii, Stanów Zjednoczonych.

www.gov.pl/web/dyplomacja/oswiadczenie-ministra-spraw-zagranicznych-rzeczypospolitej-polskiej-w-zwiazku-z-wypowiedzia-sekretarza-stanu-usa-w-sprawie-przekazania-samolotow-ukrainie [dostęp: 5.01.2023].

13 A. Gorczyca, *Medyka. Płaczący malec z filmu, który obiegł świat, nie szedł do granicy sam. Pogranicznicy sprawdzili: To 4-letni Walerij*, Gazeta Wyborcza, Rzeszów, 2022, https://rzeszow.wyborcza.pl/rzeszow/7,34962,28199741,fake-news-malec-ktory-mial-sam-przekroczyc-granice-w-medyce.html?utm_source=facebook.com&utm_medium=SM&utm_campaign=FB_Gazeta_Wyborcza&fbclid=IwAR2YoD%E2%80%93LDolulxFYesozxgqaCXmzKEDZnS61OxG34BcODdTnHOR%E2%80%93uws_6Ok [dostęp: 5.01.2023].

Źródło: https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8377943,zelenski-polski-parlament-wojna-ukraina.html [dostęp: 5.01.2023].

Fot. 9. Prezydent Ukrainy Wołodymyr Zełenski (na ekranie) przemawia podczas uroczystego zgromadzenia posłów i senatorów na sali plenarnej Sejmu w Warszawie

16 marca – do Kijowa przybyli pierwsi przywódcy innych państw. Byli to: premier Mateusz Morawiecki, wicepremier Jarosław Kaczyński oraz premier Czech Petr Fiala i premier Słowenii Janez Jansza[14].

16 marca – Rosjanie zbombardowali teatr w Mariupolu, w którym było około 1000 cywili. Obiekt był oznaczony napisem „dzieci"[15].

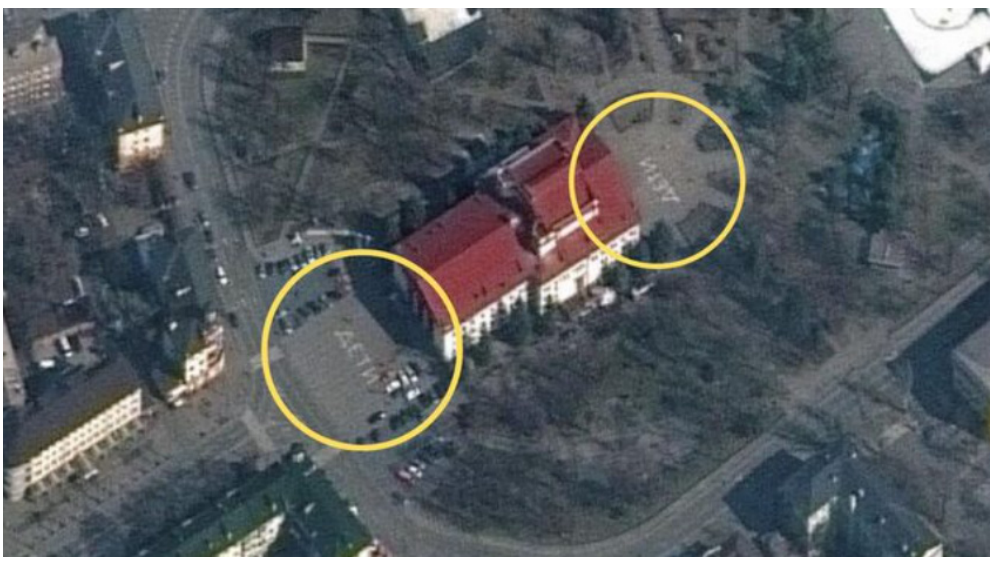
29 marca – Ukraińcy ujawnili zbrodnię w Buczy; odkryli ponad 400 ciał cywilów. Świat obiegły porażające zdjęcia rozstrzelanych mieszkańców miasta.

14 Ł. Lipiński, *„Misja pokojowa" na Ukrainie. O co chodzi Kaczyńskiemu?*, Polityka, 2022, https://www.polityka.pl/tygodnikpolityka/swiat/2158427,1,misja-pokojowa-na-ukrainie-o-co-chodzi-kaczynskiemu.read [dostęp: 5.01.2023].

15 *Wojna na Ukrainie. Rosjanie zbombardowali teatr, w którym było około tysiąca cywili. Obiekt był oznaczony napisem dzieci*, Bielsk.eu, 2022, https://bielsk.eu/kraj-swiat/37008-wojna-na-ukrainie-rosjanie-zbombardowali-teatr-w-ktorym-bylo-okolo-tysiaca-cywili-obiekt-byl-oznaczony-napisem-dzieci-foto-wideo [dostęp: 5.01.2023].

Źródło: https://www.polityka.pl/tygodnikpolityka/swiat/2158427,1,misja-pokojowa-na-ukrainie-o-co-chodzi-kaczynskiemu.read [dostęp: 5.01.2023].

Fot. 10. Wizyta premierów Polski, Czech i Słowenii w Kijowie



Źródło: https://bielsk.eu/kraj-swiat/37008-wojna-na-ukrainie-rosjanie-zbombardowali-teatr-w-ktorym-bylo-okolo-tysiaca-cywili-obiekt-byl-oznaczony-napisem-dzieci-foto-wideo [dostęp: 5.01.2023].

Fot. 11. Zbombardowany teatr w Mariupolu

Źródło: https://commons.wikimedia.org/wiki/File:Bucha_after_Russian_invasion_of_Ukraine_5.jpg [dostęp: 5.01.2023].

Fot. 12. Ofiary zbrodni w Buczy

Źródło: https://natemat.pl/404615,ludobojstwo-rosjan-w-buczy-pod-kijowem-ciala-zabitych-na-ulicach [dostęp: 5.01.2023].

Fot. 13. Ofiary zbrodni w Buczy

7 kwietnia – zespół Pink Floyd zaprezentował swoją wersję ukraińskiej piosenki „Czerwona kalina", z udziałem ukraińskiego wokalisty-żołnierza.

11 kwietnia – ukazał się raport Amnesty International Polska pt. „Polska: okrucieństwo zamiast współczucia na granicy z Białorusią", w którym krytycznie została oceniona reakcja Polski na operację specjalną reżimu białoruskiego polegającą na przepychaniu rzekomych uchodźców przez granicę Polski, Litwy i Łotwy[16].

Źródło: https://amnesty.org.pl/okrutne-traktowanie-na-granicy-polsko-bialoruskiej-i-w-osrodkach-dla-cudzoziemcow/ [dostęp: 5.01.2023].

Fot. 14. Print screen internetowej strony Amnesty International Polska

14 kwietnia – dziennikarze „Deutsche Welle" ujawnili fotomontaże internetowych filmów ukraińskich. Analiza wykazuje wiele manipulacji dotyczących m.in. zniszczeń czołgów rosyjskich i tego, że niektóre obrazy pochodzą z innych wojen, pokazano czołgi zniszczone w 2014 roku lub podczas wojny w Syrii[17].

16 *Okrucieństwo zamiast współczucia na granicy z Białorusią*, Warszawa 2022.

17 M. Trobridge, *Sprawdzenie faktów: dlaczego te osiągnięcia wojskowe Ukrainy nie są prawdziwe*, DW.com, 2022, https://www.dw.com/de/faktencheck-warum-diese-milit%C3%A4rischen-erfolge-der-ukraine-nicht-echt-sind/a-61473133 [dostęp: 5.01.2023].

Źródło: https://www.dw.com/de/faktencheck-warum-diese-milit%C3%A4rischen-erfolge-der-ukraine-nicht-echt-sind/a-61473133 [dostęp: 5.01.2023].

Fot. 15. Print screen internetowej strony „Deutsche Welle"

17 maja – ministrowie spraw zagranicznych Szwecji i Finlandii podpisali wnioski o przystąpienie ich państw do Sojuszu Północnoatlantyckiego.

Źródło: https://radioszczecin.pl/6,440388,andrzej-duda-w-kijowie-nadszedl-czas-na-nowy-pol [dostęp: 5.01.2023].

Fot. 16. Prezydent Andrzej Duda w parlamencie ukraińskim w Kijowie

22 maja – prezydent Andrzej Duda wystąpił przed parlamentem Ukrainy w Kijowie. Był on pierwszym od ataku Rosji na Ukrainę przywódcą w ukraińskim parlamencie.

Do 3 czerwca – Unia Europejska przyjęła łącznie sześć pakietów sankcji w reakcji na inwazję Rosji na Ukrainę.

6 czerwca – Elon Musk podał informację, że już 27 lutego 2022 roku przekazał Ukrainie zestawy Starlink firmy SpaceX. W sumie przekazano 15 tys. zestawów internetowych, routerów. Starlink to usługa szerokopasmowa firmy SpaceX, która nie wykorzystuje naziemnej infrastruktury, ale sieć satelitów zawieszonych na niskiej orbicie. Ukraińskie wojsko z powodzeniem wykorzystuje Starlink m.in. do koordynowania ruchu dronów[18].

17 czerwca – Ukraińcy zachwalali w mediach, sprawdzone w warunkach bojowych, polskie wyrzutnie przeciwlotnicze Piorun i produkowane w naszym kraju samobieżne haubice Krab.

1 lipca – ambasador Ukrainy w Niemczech w wywiadzie wychwalał Stepana Banderę. Został skrytykowany za to, że zasila rosyjską narrację, która ma skłócić Polaków i Ukraińców[19].

3 lipca – została opublikowana analiza przygotowana przez BBC pokazująca skalę wsparcia finansowego dla Ukrainy przez poszczególne kraje:

- Stany Zjednoczone zobowiązały się do przekazania wsparcia w wysokości 25,45 mld dolarów. Dotychczas przekazały środki na cele militarne w wysokości 6,3 mld dolarów;
- Wielka Brytania zobowiązała się do przekazania 3,73 mld dolarów, natomiast rzeczywiste dotychczasowe wydatki to 1,6 mld dolarów;
- Polska zobowiązała się do udzielenia Kijowowi wsparcia o wartości 1,81 mld dolarów;
- Niemcy zadeklarowały 1,48 mld dolarów;
- Kanada – 0,8 mld;

18 K. Duffy, *Elon Musk zdradził, ile zestawów Starlink jest w Ukrainie*, Businessinsider.com.pl, 2022, https://businessinsider.com.pl/technologie/nowe-technologie/elon-musk-zdradzil-ile-zestawow-starlink-jest-w-ukrainie/jjkh2tk [dostęp: 5.01.2023].

19 M. Zaremba, *Ambasador Ukrainy w Niemczech o Banderze i Polakach. Szybka reakcja polskiego i ukraińskiego MSZ*, Wprost.pl, 2022, https://www.wprost.pl/polityka/10766770/ambasador-ukrainy-w-niemczech-o-banderze-i-polakach-szybka-reakcja-polskiego-i-ukrainskiego-msz.html [dostęp: 5.01.2023].

– Norwegia – 0,48 mld;
– Czechy – 0,27 mld USD[20].

12 lipca – minister obrony narodowej Mariusz Błaszczak potwierdził, że wartość wsparcia wojskowego przekazanego Ukrainie przez Polskę to 1,7 mld dolarów[21].

Źródło: https://www.pap.pl/aktualnosci/news%2C1409784%2Cszef-mon-podal-wartosc-przekazanego-ukrainie-sprzetu-nie-sa-koszty-jest [dostęp: 5.01.2023].

Fot. 17. Wicepremier, minister obrony narodowej Mariusz Błaszczak

25 lipca – Rada Języka Polskiego zachęcała do stosowania połączeń: do Ukrainy (w Ukrainie), zamiast: na Ukrainę (na Ukrainie)[22].

20 *Skala pomocy dla Ukrainy. USA, W. Brytania, Polska*, wGospodarce, 2022, https://wgospodarce.pl/informacje/113946-skala-pomocy-dla-ukrainy-usa-w-brytania-polska [dostęp: 5.01.2023].

21 *Szef MON: wartość wsparcia przekazanego Ukrainie przez Polskę to 1,7 mld dolarów, jesteśmy w czołówce*, PAP, 2022, https://www.pap.pl/aktualnosci/news%2C1364989%2Cszef-mon-wartosc-wsparcia-przekazanego-ukrainie-przez-polske-17-mld [dostęp: 5.01.2023].

22 *„W Ukrainie" i „do Ukrainy" – do stosowania takiej składni zachęca Rada Języka Polskiego*, OKO.press.pl, 2022, https://oko.press/w-ukrainie-i-do-ukrainy-do-stosowania-takiej-skladni-zacheca-rada-jezyka-polskiego [dostęp: 5.01.2023].

26 lipca – żona prezydenta Ukrainy Ołena Zełenska wzięła udział w sesji fotograficznej dla „Vogue", za co została skrytykowana, że lansuje w trakcie wojny[23].

Źródło: https://kobieta.onet.pl/wiadomosci/zelenska-pozowala-dla-voguea-nie-wszyscy-sa-zadowoleni-gorzkie-slowa-internautow/pv9pll5 [dostęp: 5.01.2023].

Fot. 18. Ołena Zełenska na okładce amerykańskiego „Vogue"

23 K. Chibowska, *Ołena Zełenska pozowała dla „Vogue'a". Nie wszyscy są zadowoleni. Gorzkie słowa internautów obiegły sieć*, Onet, 2022, https://kobieta.onet.pl/wiadomosci/zelenska-pozowala-dla-voguea-nie-wszyscy-sa-zadowoleni-gorzkie-slowa-internautow/pv9pll5 [dostęp: 5.01.2023].

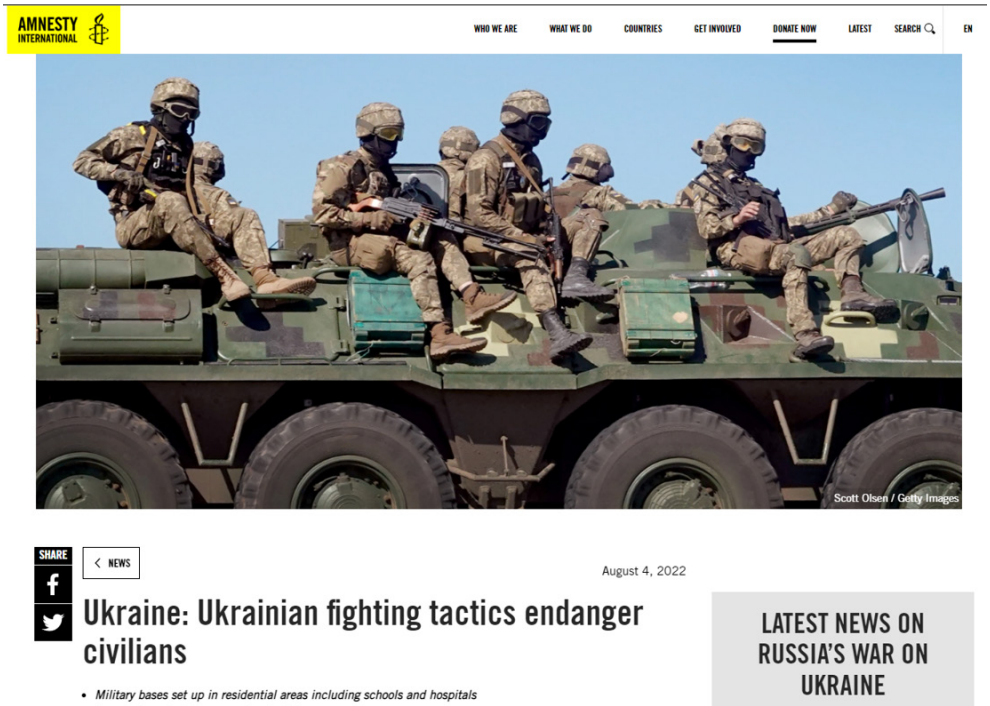
3 sierpnia – ukazał się kontrowersyjny wywiad byłego kanclerza Niemiec Gerharda Schroedera dla tygodnika „Stern", w którym były kanclerz poparł Rosję[24].

Źródło: https://www.stern.de/politik/deutschland/gerhard-schroeder---warum-soll-ich-mich-entschuldigen----32593292.html [dostęp: 5.01.2023].

Fot. 19. Print screen internetowej strony pisma „Stern"

24 B. Dudek, *Niemiecka prasa o Gerhardzie Schroederze: hochsztapler, marionetka, nadworny błazen*, Wirtualna Polska, 2022, https://wiadomosci.wp.pl/niemiecka-prasa-o-gerhardzie-schroederze-hochsztapler-marionetka-nadworny-blazen-6797793036954112a [dostęp: 5.01.2023].

4 sierpnia – Amnesty International publikowała raport, z którego wynika, że zarówno Rosja, jak i Ukraina łamią międzynarodowe prawo humanitarne. Zostało to uznane za wsparcie Rosji[25].



Źródło: https://amnesty.org.pl/ukrainska-taktyka-wojskowa-stanowi-zagrozenie-dla-ludnosci-cywilnej/ [dostęp: 5.01.2023].

Fot. 20. Print screen internetowej strony Amnesty International

6 sierpnia – Straż Graniczna podała, że od początku wojny do Polski przybyło 5,297 mln osób uciekających przed wojną w Ukrainie (równocześnie wyjechało z Polski 3,409 mln Ukraińców). Organizacja Narodów Zjednoczonych podała, że od 24 lutego Ukrainę opuściło łącznie ponad 9,9 mln osób. Na terenie Europy przebywało ponad 6,1 mln uchodźców z Ukrainy.

24 sierpnia, pół roku wojny, czyli 182 dzień wojny – prezydent Joe Biden ogłosił największy jednorazowy pakiet pomocy Białego Domu dla Ukrainy w wysokości 3 mld dolarów, odkąd rozpoczęła się rosyjska inwazja. Niemcy potwierdziły tego dnia, że sfinalizowały transport darów wojskowych o wartości 0,5 mld euro.

25 *Ukraińska taktyka wojskowa stanowi zagrożenie dla ludności cywilnej*, Warszawa 2022.

Wnioski dotyczące infrastruktury medialnej

Analiza zestawionych głównych wydarzeń – z punktu widzenia mediów – dotyczących wojny w Ukrainie pozwala wyciągnąć kilka wniosków, które mogą być przydatne do wzmacniania naszej obronności, szczególnie w dziedzinie cyberbezpieczeństwa.

Zakres definicyjny cyberbezpieczeństwa obejmuje cztery obszary, które powinny być omawiane wspólnie:

1) prawo dotyczące cyberprzestrzeni;
2) system bezpieczeństwa i instytucje odpowiedzialne za cyberbezpieczeństwo;
3) internet, rozumiany jako środowisko medialne;
4) przestrzeń internetu, która jest nowym środowiskiem społecznym[26].

Wojna pokazała, że polskie prawo dotyczące cyberprzestrzeni musi być dyskutowane i systematycznie doprecyzowywane, a cały system bezpieczeństwa i instytucje odpowiedzialne za cyberbezpieczeństwo muszą być przejrzane od nowa. W maju 2020 roku prezydent Andrzej Duda zatwierdził „Strategię bezpieczeństwa narodowego Rzeczypospolitej Polskiej", w której wskazano zagrożenie atakami hybrydowymi za strony Rosji, co wkrótce stało się faktem. Zapisano w niej: „Federacja Rosyjska prowadzi również działania poniżej progu wojny (o charakterze hybrydowym), niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także podejmuje wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych"[27].

Tuż przed atakiem kinetycznym Rosji na Ukrainę nastąpiło tzw. uderzenie hybrydowe z użyciem migrantów sprowadzanych na granicę Białorusi z krajami Unii Europejskiej. Reżim Aleksandra Łukaszenki próbował ich przepychać do Polski i na Litwę po to, żeby wywołać zamieszanie, które miało odciągnąć uwagę od przygotowań do militarnego zaatakowania Ukrainy. W pewnym stopniu to się udało, niektórzy bowiem politycy i media dały się nabrać, że mamy do czynienia z autentycznymi uchodźcami, którzy potrzebują pomocy. Wojna w Ukrainie rozpoczęła się dużo wcześniej niż atak kinetyczny, bo

26 S. Stalmach, *Cztery obszary cyberbezpieczeństwa – omówienie zakresu tematycznego*, „Przegląd Policyjny" 2021, nr 1, s. 94.
27 *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, s. 6.

inwazja rosyjska została poprzedzona działaniami paramilitarnymi na granicach Białorusi z Polską, Litwą i Łotwą.

Wojna w Ukrainie uzmysławia nam jak ważna jest infrastruktura medialna. Wbrew pozorom wojna w Ukrainie nie była w pierwszych dniach powszechnie pokazywana w mediach. Ukraińskie media nie były przygotowane do działań wojennych. Dziennikarze ukraińscy Alina Makarczuk i Ołeh Biłecki mówili w sierpniu 2022 roku na antenie TVN24 o tym, jak dowiedzieli się o wybuchu wojny[28].

Źródło: A. Makarczuk, O. Biłecki, op. cit.

Fot. 21. Print screen internetowej strony TVN24

Biłecki powiedział, że 24 lutego rano nie działała żadna informacyjna telewizja ukraińska. Ukraińcy dowiedzieli się o wojnie z telewizji rosyjskich i amerykańskich. Makarczuk dodała, że o wojnie ludzie w Ukrainie dowiadywali się z Telegramu i mediów społecznościowych. Biłecki, wówczas dziennikarz telewizji Ukraina24, przyznał, że do pracy został wezwany dopiero wieczorem 24 lutego. W innym wywiadzie dodał, że od wybuchu wojny największe

28 A. Makarczuk, O. Biłecki, *Pół roku temu Rosja zaatakowała Ukrainę. ... wspominają wybuch wojny*, TVN24, 2022, https://tvn24.pl/swiat/pol-roku-temu-rosja-zaatakowala-ukraine-dziennikarze-alina-makarczuk-i-oleh-bilecki-wspominaja-wybuch-wojny-6081689, [dostęp: 5.01.2023].

telewizje w Ukrainie połączyły siły i nadawały wspólny program – częściowo ze Lwowa[29]. Prawdopodobnie szybko także zostały zniszczone przez Rosjan nadajniki naziemne w Ukrainie. Sytuację poprawiła nieco interwencja firmy Elona Muska, który wyposażył Ukrainę w łączność satelitarną. W tym kontekście należy zadać pytanie o cały system zabezpieczenia łączności w naszym kraju, tj., jakie wnioski należy wpisać do ustawy o krajowym systemie cyberbezpieczeństwa[30], do „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej"[31], a także – być może – do zadań wojsk obrony cyberprzestrzeni?

Wnioski dotyczące propagandy i racji stanu

Propaganda była i jest bardzo ważnym elementem każdej wojny. Propagandą i dezinformacją posługują się najeźdźcy i obrońcy, a także wszyscy zaangażowani w konflikt, a nawet jedynie jego obserwatorzy. Terytorialnie wojna toczy się na konkretnych ziemiach, ale medialnie w cyberprzestrzeni wielu krajów. Bardzo wyraźnie objawiło się to podczas napaści Rosji na Ukrainę.

Na podstawie analizy wydarzeń medialnych da się wyróżnić trzy obszary aktywności propagandowej: wzmacnianie własnego morale, deprecjację obrazu przeciwnika oraz pozyskiwanie przychylności społeczeństw trzecich. Rosjanie twierdzili, że prowadzą operację specjalną, której celem jest obrona Rosji, a może i całego świata, przed ukraińskimi nazistami, odnosili się tym samym do pamięci o II wojnie światowej. Ukraińcy nazywają Rosjan orkami, czyli obrzydliwymi stworami rodem z tolkienowskich opowieści, które atakują ludzi – dziś mieszkańców Ukrainy, a jutro być może także innych krajów europejskich.

Powszechnie uważa się, że Ukraina skutecznie się broni dzięki waleczności swoich żołnierzy oraz wsparciu militarnemu i finansowemu udzielanemu przez Stany Zjednoczone, Wielką Brytanię, Polskę i inne kraje. Przy okazji jak

29 O. Biłecki, *Zełenski? To nie był prezydent z mojej bajki. Do wybuchu wojny*, rozm. J. Tacik, TVN24, 2022, https://tvn24.pl/premium/oleh-bilecki-ukrainski-dziennikarz-o-wojnie-prezydencie-wolodymyrze-zelenskim-polakach-rosjanach-i-papiezu-franciszku-wywiad-5711640 [dostęp: 5.01.2023].

30 *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. 2018, poz. 1560.

31 *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, Warszawa 2019, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 5.01.2023].

na dłoni widać różnice interesów poszczególnych państw i odmiennie prowadzoną politykę zagraniczną przez takie kraje jak: Niemcy, Francja, Chiny czy Indie.

Polska jednoznacznie, szybko i nie szczędząc środków, opowiedziała się za Ukrainą. Odbyło się to pomimo urazów istniejących pomiędzy naszymi krajami, które nie zostały dotychczas przepracowane, a które dotyczą głównie stosunku do UPA i Stepana Bandery. Dodatkowo propaganda rosyjska straszy co jakiś czas wizją aneksji części Ukrainy przez Polskę. Żywo był dyskutowany np. wywiad ambasadora Ukrainy w Niemczech, który chwalił Banderę. Ambasador został wkrótce przez rząd w Kijowie odwołany z Berlina oficjalnie za to, że dał paliwo propagandzie rosyjskiej. Jeszcze częściej na czołówki mediów dostawały się relacje opisujące zachowania rządu niemieckiego wobec potrzebującej pomocy Ukrainy. Obiektywnie, Niemcy zachowywali się niejednoznacznie – z jednej strony deklarowali pomoc, z drugiej, zwlekali z jej faktycznym przekazaniem. Subiektywnie, na stosunek polskich mediów do polityki niemieckiej wobec Ukrainy miała wpływ – wydaje się – nasza wzajemna, polsko-niemiecka rywalizacja w Unii Europejskiej i NATO.

W wyniku analizy zdarzeń medialnych widać wyraźnie, że resentymenty nadal zajmują ważne miejsce w świadomości społecznej Polaków. Napaść Rosji na Ukrainę uzmysławia nam jaką pożywką dla wrogiej propagandy i dezinformacji są nieprzepracowane animozje między państwami i społeczeństwami.

Zakończenie

Reasumując, wojna w Ukrainie rozpoczęła się długo przed atakiem kinetycznym i dotyczy także cyberprzestrzeni, która jest ponad granicami krajów. Bardzo ważnym komponentem sił obronnych są media i cała z nimi związana infrastruktura nadawcza. Walka z wrogą propagandą to nie tylko wychwytywanie dezinformacji, lecz także przepracowywanie własnych uprzedzeń oraz definiowanie racji stanu, do czego niezbędna jest współpraca mediów krajowych.

Istnieją dwie podstawowe definicje pojęcia „wojna". Na uczelniach wojskowych z pewnością rozpowszechniona jest ta, którą zapisał w swoim dziele pt. „O naturze wojny" Carl Gottlieb von Clausewitz, pruski teoretyk wojny i generał, a mianowicie: „Wojna jest tylko kontynuacją polityki innymi środkami"[32].

32 C. Clausewitz, *O naturze wojny*, Warszawa 2010, s. 46.

Zupełnie inną definicje wojny przedstawiła Hannah Arendt, niemiecka teoretyk polityki pochodzenia żydowskiego, filozofka, która uważała wręcz przeciwnie, że wojna nie jest kontynuacją polityki, a nawet zupełnym zaprzeczeniem politykowania. W książce pt. „Polityka jako obietnica" napisała: „Ponieważ wojny nie da się prowadzić bez rozkazów i posłuszeństwa, i ponieważ decyzje militarne nie mogą być przedmiotem dyskusji i perswazji, wojna należała, według Greków, do sfery niepolitycznej […]. Wojna nie jest tutaj kontynuacją polityki innymi środkami, ale czymś przeciwnym […]"[33].

Wojna w Ukrainie zmusza nas do kolejnego przemyślenia, czym są wojny, czy można ich w ogóle uniknąć i jaką rolę odgrywają media w tym kontekście.

Bibliografia

Arendt H., *Polityka jako obietnica*, Warszawa 2007.

Biłecki O., *Zełenski? To nie był prezydent z mojej bajki. Do wybuchu wojny*, rozm. J. Tacik, TVN24, 2022, https://tvn24.pl/premium/oleh-bilecki-ukrainski-dziennikarz-o-wojnie-prezydencie-wolodymyrze-zelenskim-polakach-rosjanach-i-papiezu-franciszku-wywiad-5711640 [dostęp: 5.01.2023].

*Bohaterska śmierć obrońców Wyspy Węży. Rosyjski okręcie wojenny, spie***laj*, Wprost.pl, 2022, https://www.wprost.pl/wojna-na-ukrainie/10636126/bohaterska-smierc-obroncow-wyspy-wezy-rosyjski-okrecie-wojenny-spielaj.html [dostęp: 5.01.2023].

Charmaz K., *Teoria ugruntowana. Praktyczny przewodnik po analizie jakościowej*, Warszawa 2009.

Chibowska K., *Ołena Zełenska pozowała dla „Vogue'a". Nie wszyscy są zadowoleni. Gorzkie słowa internautów obiegły sieć*, Onet, 2022, https://kobieta.onet.pl/wiadomosci/zelenska-pozowala-dla-voguea-nie-wszyscy-sa-zadowoleni-gorzkie-slowa-internautow/pv9pll5 [dostęp: 5.01.2023].

Clausewitz C., *O naturze wojny*, Warszawa 2010.

Dudek B., *Niemiecka prasa o Gerhardzie Schroederze: hochsztapler, marionetka, nadworny błazen*, Wirtualna Polska, 2022, https://wiadomosci.wp.pl/niemiecka-prasa-o-gerhardzie-schroederze-hochsztapler-marionetka-nadworny-blazen-6797793036954112a [dostęp: 5.01.2023].

Duffy K., *Elon Musk zdradził, ile zestawów Starlink jest w Ukrainie*, Businessinsider.com.pl, 2022, https://businessinsider.com.pl/technologie/nowe-technologie/elon-musk-zdradzil-ile-zestawow-starlink-jest-w-ukrainie/jjkh2tk [dostęp: 5.01.2023].

Glaser B., *Getting Started*, *„The Grounded Theory Review" 2020*, t. 19, nr 1.

Gorczyca A., *Medyka. Płaczący malec z filmu, który obiegł świat, nie szedł do granicy sam. Pogranicznicy sprawdzili: To 4-letni Walerij*, Gazeta Wyborcza, Rzeszów, 2022, https://rzeszow.wyborcza.pl/rzeszow/7,34962,28199741,fake-news-malec-ktory-mial-sam-przekroczyc-granice-w-medyce.html?utm_source=facebook.com&utm_medium=SM&utm_campaign=FB_Gazeta_Wyborcza&fbclid=IwAR2YoD%E2%80%93LDolulxFYesozxgqaCXmzKEDZnS61OxG34BcODdTnHOR%E2%80%93uws_6Ok [dostęp: 5.01.2023].

Karnowski M., *Tak, opublikowaliśmy zapis rosyjskiej pychy i rosyjskiego kłamstwa. I od razu tak to nazwaliśmy. To ważny dokument, Polacy muszą to wiedzieć*, wPolityce, 2022, https://wpolityce.pl/polityka/587569-tak-opublikowalismy-zapis-rosyjskiej-pychy-i-klamstwa [dostęp: 5.01.2023].

33 H. Arendt, *Polityka jako obietnica*, Warszawa 2007, s. 188–189.

Konecki K., *Wizualna teoria ugruntowana. Podstawowe zasady i procedury*, „Przegląd Socjologii Jakościowej" 2012, t. 7, nr 1.

Lipiński Ł., *„Misja pokojowa" na Ukrainie. O co chodzi Kaczyńskiemu?*, Polityka, 2022, https://www.polityka.pl/tygodnikpolityka/swiat/2158427,1,misja-pokojowa-na-ukrainie-o-co-chodzi-kaczynskiemu.read [dostęp: 5.01.2023].

Ławnicki T., *Tak Putin wypowiedział wojnę. Okoliczności wymagają od nas natychmiastowych działań*, NaTemat, 2022, https://natemat.pl/398711,putin-wypowiedzial-wojne-przemowienie-prezydenta-rosji [dostęp: 5.01.2023].

Makarczuk A., Biłecki O., *Pół roku temu Rosja zaatakowała Ukrainę... wspominają wybuch wojny*, TVN24, 2022, https://tvn24.pl/swiat/pol-roku-temu-rosja-zaatakowala-ukraine-dziennikarze-alina-makarczuk-i-oleh-bilecki-wspominaja-wybuch-wojny-6081689 [dostęp: 5.01.2023].

Makarewicz N., Zygiel A., Partyła M., *Tysiące migrantów przy granicy polsko-białoruskiej. Rozbili obóz w rejonie Kuźnicy*, RMF24, 2021, https://www.rmf24.pl/raporty/raport-kryzys-na-pograniczu/news-tysiace-migrantow-przy-granicy-polsko-bialoruskiej-rozbili-o,nId,5632401#crp_state=1 [dostęp: 5.01.2023].

Mersch D., *Teorie mediów*, Warszawa 2010.

Okrucieństwo zamiast współczucia na granicy z Białorusią, Warszawa 2022.

Ossowski H., *Sznur aut na wyjeździe z Kijowa. Mieszkańcy uciekają ze stolicy Ukrainy*, Wirtualna Polska, 2022, https://wiadomosci.wp.pl/sznur-aut-na-wyjezdzie-z-kijowa-ludzie-uciekaja-ze-stolicy-ukrainy-6740734577269664a [dostęp: 5.01.2023].

Oświadczenie Ministra Spraw Zagranicznych Rzeczypospolitej Polskiej w związku z wypowiedzią Sekretarza Stanu USA w sprawie przekazania samolotów Ukrainie, MSZ, Warszawa, 2022, https://www.gov.pl/web/dyplomacja/oswiadczenie-ministra-spraw-zagranicznych-rzeczypospolitej-polskiej-w-zwiazku-z-wypowiedzia-sekretarza-stanu-usa-w-sprawie-przekazania-samolotow-ukrainie [dostęp: 5.01.2023].

Platon, *Uczta*, Warszawa 1994.

Presja ma sens. BBC usunęła kłamliwy tweet uderzający w Polskę, Tysol.pl, 2022, https://www.tysol.pl/a79856-presja-ma-sens-bbc-usunela-klamliwy-tweet-uderzajacy-w-polske [dostęp: 5.01.2023].

Skala pomocy dla Ukrainy. USA, W. Brytania, Polska, wGospodarce, 2022, https://wgospodarce.pl/informacje/113946-skala-pomocy-dla-ukrainy-usa-w-brytania-polska [dostęp: 5.01.2023].

Stalmach S., *Cztery obszary cyberbezpieczeństwa – omówienie zakresu tematycznego*, „Przegląd Policyjny" 2021, nr 1.

Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej, Warszawa 2020.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Warszawa, 2019, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp: 5.01.2023].

Szef MON: wartość wsparcia przekazanego Ukrainie przez Polskę to 1,7 mld dolarów, jesteśmy w czołówce, PAP, 2022, https://www.pap.pl/aktualnosci/news%2C1364989%2Cszef-mon-wartosc-wsparcia-przekazanego-ukrainie-przez-polske-17-mld [dostęp: 5.01.2023].

Trobridge M., *Sprawdzenie faktów: dlaczego te osiągnięcia wojskowe Ukrainy nie są prawdziwe*, DW.com, 2022, https://www.dw.com/de/faktencheck-warum-diese-milit%C3%A4rischen-erfolge-der-ukraine-nicht-echt-sind/a-61473133 [dostęp: 5.01.2023].

Ukraińska taktyka wojskowa stanowi zagrożenie dla ludności cywilnej, Warszawa 2022.

„W Ukrainie" i „do Ukrainy" – do stosowania takiej składni zachęca Rada Języka Polskiego, OKO.press.pl, 2022, https://oko.press/w-ukrainie-i-do-ukrainy-do-stosowania-takiej-skladni-zacheca-rada-jezyka-polskiego [dostęp: 5.01.2023].

Wojna na Ukrainie. Gdzie toczą się kluczowe walki?, Polskie Radio Program Trzeci, Warszawa, 2022, https://trojka.polskieradio.pl/artykul/2909545,Wojna-na-Ukrainie-Gdzie-tocza-sie-kluczowe-walki-POSLUCHAJ [dostęp: 5.01.2023].

Wojna na Ukrainie. Rosjanie zbombardowali teatr, w którym było około tysiąca cywili. Obiekt był oznaczony napisem dzieci, Bielsk.eu, 2022, https://bielsk.eu/kraj-swiat/37008-wojna-na-ukrainie-rosjanie-zbombardowali-teatr-w-ktorym-bylo-okolo-tysiaca-cywili-obiekt-byl-oznaczony-napisem-dzieci-foto-wideo [dostęp: 5.01.2023].

Zaremba M., *Ambasador Ukrainy w Niemczech o Banderze i Polakach. Szybka reakcja polskiego i ukraińskiego MSZ*, Wprost.pl, 2022, https://www.wprost.pl/polityka/10766770/ambasador-ukrainy-w-niemczech-o-banderze-i-polakach-szybka-reakcja-polskiego-i-ukrainskiego-msz.html [dostęp: 5.01.2023].

Polish media about the war in Ukraine – an overview of the most important events of the first half of 2022

Abstract

The war that Russia has been waging against Ukraine since 2022 is brutal and described as full-scale, i.e. with the use of all forces and means. In the era of dynamically developing media, information has also become a weapon that is consciously used in this conflict.

When reviewing the most important information that was the focus of interest of a large part of the media in Poland during the first half of the year after the Russian attack on Ukraine, it can be stated that the media in Poland extensively inform about the war in Ukraine, but they do not limit themselves to reporting the conflict, they also refer to to disinformation and propaganda, and even touch on the sphere of resentment that is still alive between different countries. The summary of information makes it clear how important the media are in the modern world and that care for their development and securing the media infrastructure is a strategic task of the state.

Key words: media, war in Ukraine, cybersecurity, disinformation

Jacek Sobczak*
Ksenia Kakareko**
Maria Gołda-Sobczak***

Poszukiwanie unijnych standardów sztucznej inteligencji

Streszczenie

Cyberbezpieczeństwo jest ściśle związane z kwestią sztucznej inteligencji. Punktem wyjścia do jej prezentacji w perspektywie unijnej jest komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy"[1]. Poprzedziła go opinia Europejskiego Komitetu Ekonomiczno-Społecznego opracowana z inicjatywy własnej tego Komitetu „Sztuczna inteligencja: wpływ sztucznej inteligencji na jednolity rynek (cyfrowy), produkcję, konsumpcję, zatrudnienie i społeczeństwo"[2]. W treści tej opinii Europejski Komitet Ekonomiczno-Społeczny skonstatował, że nie istnieje powszechnie przyjęta, precyzyjna definicja sztucznej inteligencji[3].

Słowa kluczowe: sztuczna inteligencja, rynek cyfrowy, nowe technologie

* Prof. dr hab. nauk prawnych Jacek Sobczak, sędzia Sądu Najwyższego w stanie spoczynku, Instytut Nauk Prawnych, Akademia Ekonomiczno-Humanistycznej w Warszawie, ORCID 0000-0002-2231-8824.
** Dr hab. nauk prawnych Ksenia Kakareko, Katedra Prawa Mediów, Wydział Dziennikarstwa, Informacji i Bibliologii, Uniwersytet Warszawski, ORCID: 0000-0003-3707-4479.
*** Dr hab. nauk społecznych Maria Gołda-Sobczak, prof. UAM, Instytut Kultury Europejskiej, Uniwersytet im. Adama Mickiewicza w Poznaniu, ORCID: 0000-0002-3854-7007.

1 COM (2018) 237 final.

2 Dz. Urz. UE 2017, C 28, s. 1. Opinia została przygotowana przez Sekcję Jednolitego Rynku, Produkcji i Konsumpcji, który przyjął ją 4 maja 2017 r. Zgromadzenie Plenarne Europejskiego Komitetu przyjęło tę opinię 31 maja 2017 r. na 526 sesji plenarnej przytłaczającą większością 159 głosów „za", trzech głosach sprzeciwu i 14 wstrzymujących się. Sprawozdawcą była Catelijne Muller.

3 W treści opinii wskazano, że pojęcie to obejmuje wiele poddziedzin takich, jak: „ucząca się" architektura systemów obliczeniowych (*cognitive computing* – algorytmy rozumujące

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy" z 25 kwietnia 2018 roku

W komunikacie Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy" z 25 kwietnia 2018 roku[4] stwierdzono, że termin „sztuczna inteligencja" odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – do osiągnięcia konkretnych celów. Systemy sztucznej inteligencji mogą być oparte na oprogramowaniu, działać w świecie wirtualnym (np. asystenci głosowi, oprogramowanie do analizy obrazu, wyszukiwarki, systemy rozpoznawania mowy i twarzy) lub mogą być wbudowane w urządzenia (np. zaawansowane roboty, samochody autonomiczne, drony lub aplikacje internetu rzeczy). Unia Europejska powinna przyjąć skoordynowane podejście, żeby jak najlepiej wykorzystać możliwości, jakie oferuje sztuczna inteligencji oraz w celu sprostania nowym wyzwaniom, jakie ze sobą niesie. Unia Europejska już na zawsze może objąć przodownictwo w rozwijaniu i wykorzystywaniu sztucznej inteligencji na podstawie swoich wartości i mocnych stron[5].

Głosząc rozpoczęcie europejskiej inicjatywy w sprawie sztucznej inteligencji, przypomniano, że w maju 2017 roku Komisja opublikowała śródokresowy przegląd strategii na rzecz jednolitego rynku cyfrowego[6]. W treści tego dokumentu stwierdzono, że urzeczywistnienie jednolitego rynku cyfrowego Unii Europejskiej wymaga również przejrzystego, stabilnego środowiska prawnego stymulującego innowacje, przeciwdziałającego rozdrobnieniu rynku oraz pozwalającego wszystkim zaangażowanym podmiotom na włączanie

i rozumiejące na wyższym, tzn. bardziej ludzkim poziomie), uczenie maszynowe (algorytmy same uczące się wykonywać zadania), rozszerzona inteligencja (*augmented intelligence* – współpraca między człowiekiem i maszyną), robotyka oparta na sztucznej inteligencji (sztuczna inteligencja wbudowana w roboty).

4 COM (2018) 237 final; SWD (2018) 137 final.

5 Wskazano, że w tym celu Unia Europejska może wykorzystać światowej klasy uczonych, laboratoria i przedsiębiorstwa typu start-up, jednolity rynek cyfrowy, bogactwo danych dotyczących przemysłu, badań i sektora publicznego.

6 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „W sprawie przeglądu śródokresowego realizacji strategii jednolitego rynku cyfrowego. Połączony jednolity rynek cyfrowy dla wszystkich", Bruksela, 10 maja 2017 r., COM (2017) 228 final; SWD (2017) 155 final.

się w nową dynamikę rynku na sprawiedliwych, zrównoważonych warunkach. Stworzy to fundament ważnego w działalności gospodarczej zaufania, w tym zaufania ze strony konsumentów. Przypomniano, że taki był cel jednolitego rynku cyfrowego[7] i wskazano, że taką rolę odegra cyfryzacja w wykształceniu Europy. Podkreślono także w białej księdze sprawy przyszłości Europy[8].

7 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Strategia jednolitego rynku cyfrowego dla Europy", Bruksela, 6 maja 2015 r., COM (2015) 192 final; SWD (2015) 100 final. W treści dokumentu stwierdzono, że globalna gospodarka staje się szybko gospodarką cyfrową, a technologie komunikacyjne nie stanowią już osobnego sektora, lecz są fundamentem wszystkich nowoczesnych, innowacyjnych systemów gospodarczych. Jednolity rynek cyfrowy, jak wskazano, to przestrzeń, w której jest zapewniany swobodny przepływ towarów, osób, usług i kapitału, a obywatele i przedsiębiorstwa mogą bez przeszkód i na zasadach uczciwej konkurencji uzyskać dostęp do usług online lub je świadczyć. Wskazano, że strategia jednolitego rynku cyfrowego będzie opierać się na trzech filarach, tj.: na lepszym dostępie konsumentów i przedsiębiorstw do towarów i usług w internecie w całej Europie; na tworzeniu odpowiednich warunków do rozwoju sieci i usług cyfrowych; na maksymalizacji wzrostu gospodarczego generowanego przez europejską gospodarkę cyfrową. Podkreślono, że jednym z warunków lepszego dostępu online są nowoczesne, bardziej europejskie ramy prawa autorskiego, dlatego zadeklarowano, że do końca 2015 r. Komisja złoży wnioski ustawodawcze mające na celu zmniejszenie różnic między krajowymi systemami prawa autorskiego oraz umożliwiające użytkownikom w całej Unii powszechny dostęp do utworów. Obiecano także przeprowadzenie przeglądu dyrektywy o audiowizualnych usługach medialnych, zwrócono uwagę na jej zakres oraz na środki promujące utwory europejskie. Podkreślono rolę platform internetowych, m.in.: wyszukiwarek, mediów społecznościowych, platform handlu zagranicznego, sklepów z aplikacjami oraz porównywarek cen. Podkreślono konieczność zwalczania nielegalnych treści w internecie oraz potrzebę budowania gospodarki opartej na danych, widząc w tych wszystkich czynnikach podstawy budowy cyfrowego społeczeństwa, którego elementem będzie e-administracja. Do komunikatu dołączono załącznik zawierający harmonogram tworzenia jednolitego rynku cyfrowego.

8 Biała księga w sprawie przyszłości Europy „Refleksje i scenariusze dla UE 27 do 2025 r.", Bruksela, 1 marca 2017, COM (2017) 2025 final. W treści tego dokumentu zwrócono uwagę na siły napędowe dla przyszłości Europy i przewidziano głębokie zmiany gospodarcze i społeczne. Wskazano także najważniejsze zagrożenia i obawy dotyczące bezpieczeństwa i ochrony granic oraz kwestionowanie zaufania i legitymacji demokratycznej. Przy tej okazji podkreślono, że obywatelom nie wytłumaczono wystarczająco dobrze za co odpowiada Unia, a za co organy krajowe. Zwrócono uwagę, że istnieją rozbieżności między oczekiwaniami a zdolnością Unii do ich zaspokojenia. Podkreślono, że w poszczególnych państwach Unii istnieje tendencja do obwiniania Brukseli za problemy i jednocześnie uznawanie jej działań za swoje sukcesy w polityce krajowej. Brak odpowiedzialności za wspólne decyzje oraz nawyk szukania winnych gdzie indziej, obojętność i nieufność wobec działań podejmowanych przez organy publiczne stworzyło pustkę, którą łatwo wypełniła populistyczna i nacjonalistyczna retoryka. W dalszej części dokumentu przedstawiano pięć scenariuszy dla Europy do 2025 r. Należy żałować, że te scenariusze, podobnie jak większość dokumentów unijnych o nienormatywnym charakterze, nie jest w Polsce znana nie tylko większemu gronu społeczeństwa, lecz także większości dziennikarzom, publicystom, politologom, a nawet specjalistom badającym stosunki międzynarodowe.

Wywiedziono, że technologia cyfrowa wpłynie na każdy aspekt polityki unijnej, zauważono, że infrastruktura cyfrowa musi być solidna, odporna i zdolna do przystosowania się do zmieniających się zagrożeń. Warunkiem jest dostępny dla wszystkich internet, tworzenie środowiska przyjaznego innowacjom oraz zapewnienie rzeczywistej ochrony prywatności oraz danych osobowych w internecie. Wszystko to zmierza do zapewnienia sprawiedliwego, otwartego i bezpiecznego otoczenia cyfrowego. W dalszej części dokumentu podjęto problem strategii bezpieczeństwa cybernetycznego Unii. Podkreślono, że istnieje konieczność przeglądu tych dokumentów. Jako ważny element wskazano kształtowanie umiejętności cyfrowych[9].

W komunikacie z 25 kwietnia 2018 roku „Sztuczna inteligencja dla Europy" wskazano, że celem europejskiej inicjatywy w sprawie sztucznej inteligencji jest zwiększenie potencjału technologicznego Unii oraz wdrożenie sztucznej inteligencji w całej gospodarce zarówno w systemie prawnym, jak i publicznym. Celem jest ponadto przygotowanie się na zmiany społeczno-gospodarcze wywołane przez sztuczną inteligencję, a także zapewnienie odpowiednich zasad etycznych i prawnych opartych na wartościach Unii i zgodnych z Kartą praw podstawowych Unii Europejskiej. Zadeklarowano zwiększenie potencjału technologicznego i przemysłowego Unii Europejskiej oraz wdrożenie sztucznej inteligencji w całej gospodarce, a także wspieranie przez Komisję technologii sztucznej inteligencji zarówno w badaniach podstawowych, jak i przemysłowych. Zauważono konieczność zapewnienia dostępu do sztucznej inteligencji wszystkim potencjalnym użytkownikom, w szczególności małym i średnim przedsiębiorcom. Podkreślono konieczność przygotowania całego społeczeństwa do zmian społeczno-gospodarczych, jakie zaistnieją w wyniku rozpowszechnienia sztucznej inteligencji. Duży nacisk położono w dokumencie na kwestie zapewnienia odpowiednich zasad etycznych i prawnych oraz stworzenie atmosfery zaufania do rozwoju i odpowiedzialności za niego oraz

9 Przywołano w tej kwestii Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Nowy europejski program na rzecz umiejętności. Wspólne działania na rzecz wzmocnienia kapitału ludzkiego, zwiększania szans na zatrudnienie i konkurencyjności", Bruksela 22 września 2016, COM (2016) 381 final/2; SWD (2016) 195 final. Ważną częścią dokumentu jest kwestia umiejętności cyfrowych. Stwierdzono, że Komisja jest w trakcie uruchamiania inicjatywy „Koalicja na rzecz umiejętności cyfrowych i zatrudnienia" i wezwano państwa członkowskie, żeby do połowy 2017 r. opracowały kompleksową krajową strategię w zakresie umiejętności cyfrowych. Na marginesie należy wskazać koncepcję modernizacji szkolnictwa wyższego i nawiązanie do planu modernizacji europejskich systemów szkolnictwa wyższego. Zob. COM (2011) 567 final.

stosowania sztucznej inteligencji. Wskazano, że jest to konieczne, ponieważ zarówno obywatele, jak i przedsiębiorstwa muszą zaufać technologiom, z którymi się stykają, i móc żyć w przewidywalnym i zrozumiałym otoczeniu prawnym, polegać na skutecznych zabezpieczeniach chroniących ich podstawowe prawa i wolności. Pierwszym krokiem w kierunku rozwiązania problemów etycznych miało być opracowanie do końca 2018 roku projektów dotyczących etyki sztucznej inteligencji. Wytyczne te miały się opierać na pracach Europejskiej Grupy ds. Etyki w Nauce i Nowych Technologiach, będącej ciałem doradczym Komisji. Warto wspomnieć, że 9 marca 2018 roku opublikowała ona stosowne oświadczenie w sprawie sztucznej inteligencji, robotyki i systemów autonomicznych[10]. Wskazała, że pierwszym krokiem może być samoregulacja, ale organy publiczne muszą zapewnić zgodność dokumentów regulacyjnych dotyczących rozwoju i stosowania technologii sztucznej inteligencji z wartościami i prawami podstawowymi. Zauważono, że pojawienie się sztucznej inteligencji wymaga zastanowienia się nad adekwatnością niektórych przepisów dotyczących bezpieczeństwa oraz kwestii odpowiedzialności cywilnoprawnej[11].

Zadeklarowano, że zmierzając do przygotowania obywateli do najlepszego wykorzystania sztucznej inteligencji, Komisja postanowiła ustanowić do końca 2018 roku dla zainteresowanych stron i ekspertów europejskiego sojuszu na rzecz sztucznej inteligencji wskazówki do projektów wytycznych dotyczących etyki sztucznej inteligencji, które powinny być opracowane we współpracy z Europejską Grupą Etyki ds. Nauki i Nowych Technologii z należytym poszanowaniem praw podstawowych. Ponadto Komisja zobowiązała się opublikować w pierwszej połowie 2019 roku wytyczne dotyczące interpretacji dyrektywy w sprawie odpowiedzialności za produkt w świetle postępu technologicznego.

10 Problemów etycznych dotyczących sztucznej inteligencji dotykają dokumenty międzynarodowe: zasady dotyczące sztucznej inteligencji z Asilomar (https://futureoflife.org/ai-principles/ [dostęp: 3.10.2022]), deklaracja z Montrealu w sprawie odpowiedzialnej sztucznej inteligencji (https://www.montrealdeclaration-responsibleai.com/ [dostęp: 3.10.2022]), 10 najważniejszych zasad dotyczących etycznej sztucznej inteligencji opracowanych przez UNI Global Union (http://www.thefutureworldofwork.org/opinions/10-principles-for-ethical-ai/ [dostęp: 3.10.2022]). Prace w tym zakresie prowadzi także międzynarodowy dialog Komisji Europejskiej w dziedzinie bioetyki i etyki w nauce i nowych technologiach, który skupia krajowe rady ds. etyki państw członkowskich Unii Europejskiej i krajów trzecich w celu współpracy w kwestiach będących przedmiotem wspólnego zainteresowania.

11 Przywołano dokument służb Komisji Odpowiedzialności związanych ze sztuczną inteligencją i nowymi technologiami towarzyszącymi Commission Staff Working Document Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Maximising the Benefits of Articificial Intelligence for Europe [SWD (2018) 137 final].

Do połowy 2019 roku zadeklarowano opublikowanie sprawozdania na temat skutków, potencjalnych luk oraz kierunków rozwoju, a także odpowiedzialności i bezpieczeństwa w aspekcie internetu rzeczy i robotyki. Postanowiono także wspierać badania nad wyjaśnianiem sztucznej inteligencji i wdrożyć projekt pilotażowy i zaproponowany przez Parlament Europejski dotyczący budowania świadomości algorytmów[12]. Zadeklarowano także zbieranie informacji o krajowych i unijnych organizacjach konsumenckich i organach nadzorujących ochronę danych w zrozumieniu aplikacji wykorzystujących sztuczną inteligencję. Obiecano, że do końca lipca 2018 roku zostanie utworzony Europejski Sojusz na rzecz Sztucznej Inteligencji.

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego

Komunikat Komisji „Sztuczna inteligencja dla Europy" został zaopiniowany przez Europejski Komitet Ekonomiczno-Społeczny. W przyjętej 19 września 2018 roku opinii[13] stwierdzono, że ma on na celu wzmocnienie potencjału przemysłowego i technologicznego Unii Europejskiej oraz zachęcanie do rozpowszechniania sztucznej inteligencji w całej europejskiej przeglądarce zarówno w sektorze prywatnym, jak i w administracji publicznej. Przywołując opinię wydaną z własnej inicjatywy[14], stwierdzono, że Europejski Komitet popiera inicjatywę Komisji, która zawarła w swoim komunikacie sporo wcześniejszych sugestii Komitetu i jednocześnie wezwała Komisję do szybkiego i zdecydowanego działania. W opinii stwierdzono, że przyjęcie skutecznego podejścia europejskiego do sztucznej inteligencji stanowi zachętę do znacznych inwestycji w badania i innowacje, w tym infrastruktury cyfrowe konieczne do przygotowania się na poważne wyzwania społeczno-gospodarcze, które w nadchodzących latach staną się udziałem europejskiego społeczeństwa i rynków za sprawą postępu technologicznego. Podkreślono, że na poziomie europejskim w zakresie sztucznej inteligencji muszą zostać zatwierdzone

12 https://ec.europa.eu/digital-single-market/en/algorithmic-awareness-building [dostęp: 3.10.2022].

13 Dz. Urz. UE 2018, C 440, s. 51. Opinia została przygotowana przez Sekcję Jednolitego Rynku, Produkcji i Konsumpcji, który przyjął ją 4 września 2018 r. Zgromadzenie Plenarne Europejskiego Komitetu przyjęło tę opinię 19 września 2018 r. na 537 sesji plenarnej przytłaczającą większością 199 głosów „za", jednym głosie sprzeciwu i dwóch wstrzymujących się. Sprawozdawcą była Giuseppe Guerini, współsprawozdawcą – Gonçalo Lobo Xavier.

14 Dz. Urz. UE 2017, C 28, s. 1.

zharmonizowane podstawy prawne zgodnie z Kartą praw podstawowych Unii Europejskiej i zasadami ujętymi w unijnych traktatach. Nowe podstawy regulacyjne – według opinii – powinny zawierać dokładne przepisy dotyczące zagrożeń, jakie niesie za sobą uczenie się maszyn, brak przejrzystości na rynku, brak konkurencji, dyskryminacja, nieuczciwe praktyki handlowe, zagrożenia dla cyberbezpieczeństwa i bezpieczeństwa produktu. Zabezpieczenia regulacyjne powinny być w szczególności rygorystyczne w sytuacjach, gdy systemy wykorzystujące sztuczną inteligencję automatycznie pobierają dane podczas wykorzystywania urządzeń elektronicznych i komputerów. Zauważono, że w dokumencie roboczym Komisji, który towarzyszy jej komunikatowi, analizowano wpływ sztucznej inteligencji na prawodawstwo Unii Europejskiej i określono wyzwania dotyczące odpowiedzialności powstające w kontekście technologii cyfrowej[15]. Podkreślono, że będą potrzebne kompleksowe plany działania, żeby wesprzeć modernizację systemów kształcenia i szkolenia przez rozwijanie nowych umiejętności zgodnie z wymaganiami przyszłego rynku pracy. Za konieczne uznano także zagwarantowanie wysokiego poziomu ochrony obywateli i pracowników przed oczekiwanymi wyzwaniami[16].

W odniesieniu do określonego przez Komisję celu, tj. udostępnienia sztucznej inteligencji wszystkim potencjalnym użytkownikom, Europejski Komitet uważa, że do sprostania tym wyzwaniom konieczne jest zapewnienie dostępu do sztucznej inteligencji jak największej liczbie podmiotów. Komitet uznał, że najważniejsze jest to, żeby Unia Europejska wspierała rozwój sztucznej inteligencji i zadbała o to, żeby prywatność osób fizycznych i odpowiedzialne przetwarzanie ich danych regulowały odpowiednie przepisy. Ponadto wskazała, że koniecznie należy dostosować do nowych scenariuszy, wynikających z zastosowania sztucznej inteligencji, odpowiednich już istniejących przepisów. Podniosła także konieczność pogłębiania wiedzy i kształtowania umiejętności potrzebnych ludziom, administracji i przedsiębiorstwom europejskim do skutecznego korzystania ze sztucznej inteligencji. Podkreślono, że sprawą ważną dla obywateli Unii jest otrzymanie odpowiedniego przeszkolenia i uzyskiwanie prostych oraz zrozumiałych informacji, które umożliwią im stać się

15 Zob. SWD (2018) 137 final.

16 Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Koncepcje UE dotyczące zarządzania przemianami w cyfrowym świecie pracy – zasadniczy wkład w opracowanie Białej księgi na temat przyszłości pracy" (opinia rozpoznawcza na wniosek prezydencji austriackiej), Dz. Urz. UE 2018, C 367, s. 15.

odpowiedzialnymi i świadomymi użytkownikami urządzeń i aplikacji dostępnych dzięki szybkiemu, coraz powszechniejszemu postępowi technologicznemu.

Wskazano wreszcie, że Komisja Europejska będzie musiała przeprowadzić dokładną ocenę wpływów sztucznej inteligencji na rynek pracy. Badanie to musi przy tym uwzględniać zarówno możliwe zastąpienie niektórych pracowników przez urządzenie elektroniczne lub roboty, jak i to, że pewne funkcje, choć nie zostaną w pełni zautomatyzowane, to pod wpływem nowych technologii ulegną głębokim zmianom. Zauważono, że wprowadzenie do przedsiębiorstw nowych technologii wymaga wprowadzenia dialogu społecznego między różnymi zaangażowanymi partnerami, dlatego należy informować organizacje pracownicze i związki zawodowe oraz konsultować się z nimi.

Sztuczna inteligencja jest technologią i społeczną innowacją zdolną do radykalnego przekształcenia całego społeczeństwa oraz do zmiany na lepsze zarówno sektora publicznego, jak i relacji między obywatelami a administracją publiczną. Jednakże pracownicy służby cywilnej powinni być przygotowani na zmierzenie się z wyzwaniami, jakie sztuczna inteligencja wywoła w społeczeństwie europejskim. W opinii podkreślono, że wyzwanie dla administracji publicznej jest szczególnie trudne, gdyż potrzebne jest zachowanie właściwej równowagi między interesem publicznym a indywidualnym. Trzeba szczególnie pogodzić zasadę przejrzystości i publikacji dokumentów administracyjnych z ochroną danych osobowych i prawem jednostki do prywatności w jasnych i wyraźnych przepisach regulacyjnych. Podkreślono, że organizacje społeczeństwa obywatelskiego i przedsiębiorstwa mają do odegrania ważną rolę w zwiększaniu zrozumienia i akceptacji technologii przez obywateli. Szczególne znaczenie ma, jak zauważono, możliwość tworzenia systemu partycypacyjnego sprawowania rządów, np. w formie opartej na współpracy. Stwierdzono ponadto, że organy administracyjne odpowiedzialne za mechanizmy nadzoru rynkowego powinny dysponować specjalistyczną wiedzą i uprawieniami pozwalającymi na ochronę uczciwej konkurencji, praw konsumentów, a także bezpieczeństwa i praw pracowników. Odpowiedzialność za przeprowadzanie audytów algorytmów powinna spoczywać na organach publicznych lub niezależnych podmiotach. Jednocześnie przedsiębiorstwa powinny wprowadzić skuteczne mechanizmy wykorzystywania danych przez sztuczną inteligencję.

Opinia Europejskiego Komitetu Regionów

Komunikat „Sztuczna inteligencja dla Europy" został także zaopiniowany przez Europejski Komitet Regionów[17]. W opinii tej zgodzono się ze stanowiskiem Komisji co do przełomowej zmiany związanej z nadejściem sztucznej inteligencji. Podkreślono, że sytuacja ta jest początkiem przemiany europejskiej gospodarki i społeczeństwa. Podzielono pogląd, że decydenci polityczni muszą zapewnić warunki dotyczące funkcjonowania sztucznej inteligencji, a także opracować zasady etyczne. Konieczna jest także ściślejsza koordynacja różnych obszarów polityki i programów Unii Europejskiej. Zauważono, że władze lokalne i regionalne powinny przyczyniać się do tworzenia warunków do zwiększenia inwestycji w sztuczną inteligencję. Jednakże musi to iść w parze z przystosowaniem podstaw prawnych i określeniem interakcji z usługami publicznymi oraz ze szkoleniem pracowników, przedsiębiorców, administracji i ogółu społeczności. W opinii przypomniano o zobowiązaniach dotyczących administracji elektronicznej zawartych w deklaracji z Tallina[18]. Wskazano, że zastosowanie sztucznej inteligencji w e-administracji może poprawić w całej Unii skuteczność, przejrzystość i dostęp do usług publicznych. Zauważono wreszcie, że sztuczną inteligencję oraz powiązane z nią inwestycje w przełomowe innowacje należy traktować poważnie na najwyższym szczeblu politycznym, gdyż przyczyni się to do poprawy konkurencyjności Europy i dobrobytu jej mieszańców. Wyrażono ubolewanie, że proponowana strategia nie jest wiążąca dla państw członkowskich, gdyż sztuczna inteligencja odgrywa niezmiernie ważną rolę w generowaniu wzrostu gospodarczego. Podkreślono, że należy opracować bardziej elastyczne mechanizmy wdrożenia sztucznej inteligencji i finansowania związanych z nią innowacji. Zwrócono uwagę na potrzebę wzmocnienia współpracy międzyregionalnej za pośrednictwem strategii inteligentnej specjalizacji. W opinii poparto propozycję utworzenia platformy sztucznej inteligencji „na żądanie". Podkreślono, że należy zapewnić władzom regionalnym i lokalnym możliwość przekwalifikowania oraz odpowiednie środki finansowe na organizowanie przekwalifikowania pracowników w takich miejscach pracy, które zostaną przekształcone lub zlikwidowane wraz z zastosowaniem sztucznej inteligencji. Podkreślono, że sztuczna inteligencja

17 Opinia Europejskiego Komitetu Regionów – sztuczna inteligencja dla Europy, Dz. Urz. UE 2019, C 168, s. 11.

18 Deklaracja z Tallina w sprawie administracji elektronicznej została podpisana na posiedzeniu ministerialnym 6 października 2017 r. podczas estońskiej prezydencji Rady UE.

nie jest celem samym w sobie, lecz musi być dostosowana do administracji elektronicznej i usług publicznych. Podkreślono potrzebę zagwarantowania ochrony prywatności i dóbr osobistych.

Opinia Europejskiego Komitetu Ekonomiczno-Społeczny o „Wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program »Cyfrowa Europa« na lata 2021–2027"

Europejski Komitet Ekonomiczno-Społeczny 17 października 2018 roku na 538 sesji plenarnej wydał opinię o „Wniosku dotyczącym rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program »Cyfrowa Europa« na lata 2021–2027"[19]. Opinia dotyczy wydanego 6 czerwca 2018 roku rozporządzenia w sprawie programu „Cyfrowa Europa" na lata 2021–2027. Programem tym Komisja chciała wspomóc strategię jednolitego rynku cyfrowego i wypełnić lukę inwestycyjną solidnym wsparciem finansowym. Całkowity budżet programu został określony na 9,2 mld euro. Ogólnym celem programu jest wsparcie transformacji cyfrowej przemysłu. Założono przy tym, że korzyści związane z transformacją cyfrową powinny zostać zwiększone i stać się udziałem wszystkich obywateli Europy, administracji publicznych i przedsiębiorstw w Unii Europejskiej. W opinii przypomniano, że program „Cyfrowa Europa" obejmuje pięć najważniejszych dziedzin: obliczenia wielkiej skali[20], sztuczna inteligencja[21], cyberbezpieczeństwo i zaufanie[22], zaawansowane

19 Dz. Urz. UE 2019, C 62, s. 292. Opinia została przyjęta większością 212 głosów „za", przy dwóch głosach wstrzymujących się i bez głosów sprzeciwu. Tekst został przygotowany przez Sekcję Transportu, Energii, Infrastruktury i Społeczeństwa. Sprawozdawcą był Norbert Kluge, a współsprawozdawcą – Ulrich Samm.

20 W tej dziedzinie zaplanowano, że za pomocą tzw. superkomputerów mają zostać stworzone zdolności umożliwiające lepsze przetwarzanie stale rosnących ilości danych.

21 Komisja Europejska zaplanowała 2,5 mld euro na sztuczną inteligencję. Środki te mają być wykorzystane na stworzenie i wzmocnienie zdolności Unii Europejskiej w tej dziedzinie. Podkreślono, że chodzi tu również o umożliwienie tworzenia i przechowywania dużych zbiorów danych i algorytmów oraz bezpiecznego do nich dostępu. Wskazano, że wzmocnione mają być także istniejące w państwach członkowskich placówki prowadzące testy i doświadczenia związane ze sztuczną inteligencją. Założono wspieranie współpracy między nimi.

22 Dziedzina „cyberbezpieczeństwo i zaufanie" powinna – według programu – zapewnić Unii posiadanie technologicznych i przemysłowych zdolności do zabezpieczenia swojej gospodarki, społeczeństwa i demokracji. Wskazano, że chodzi o to, żeby wspólnie z państwami członkowskimi pozyskać zaawansowane urządzenia i narzędzia służące

umiejętności cyfrowe[23], zagwarantowanie powszechnego użycia technologii cyfrowej w każdej gospodarce i w całym społeczeństwie[24]. Ponadto program zajmuje się cyfryzacją przemysłu.

W opinii z zadowoleniem przyjęto opracowanie przez Komisję Europejską programu „Cyfrowa Europa". Skonstatowano, że celem tego programu jest umożliwienie powstania jednolitego rynku cyfrowego i korzystne ukształtowanie transformacji cyfrowej w interesie wszystkich obywateli Europy. Wywiedziono, że w pierwszym rzędzie uczeni stymulują rozwój społeczny i gospodarczy. Ich wiedza i umiejętności są niezbędne do osiągnięcia wysokiego poziomu badań oraz do praktycznej realizacji programu. Zauważono, że konieczne jest zintensyfikowanie dialogu między uczonymi, partnerami społecznymi a organizacjami społeczeństwa obywatelskiego. Sugerowano, żeby program „Cyfrowa Europa" powiązać z zasadami wspierania badań naukowych w ramach programu „Horyzont 2020" („Horyzont Europa"). Zwrócono uwagę na Europejską Kartę Naukowca oraz na zasady prowadzenia odpowiedzialnych badań naukowych i innowacji oraz tzw. otwartą naukę. Pozytywnie oceniono to, że promowanie umiejętności cyfrowych podniesiono do rangi i istoty programu. Jako godne pożałowania odnotowano to, że budżet na tę priorytetową dziedzinę jest relatywnie niski. Wskazano, że program „Cyfrowa Europa" powiedzie się tylko wówczas, gdy będzie traktowany jako program naczelny i wspomagany innymi unijnymi programami o podobnych celach. W opinii podniesiono, że w tworzenie centrów innowacji cyfrowych powinni być angażowani partnerzy społeczni oraz społeczeństwo obywatelskie. Powinni oni uzyskać dostęp do centrów innowacji cyfrowych. Jako organizacje pozarządowe mogą upowszechniać działania tych centrów i przyczyniać się do ich lepszej akceptacji w społeczeństwie. Zauważono, że Europejski Komitet chciałby zawczasu zapobiegać możliwemu kryzysowi społecznemu podczas realizacji programu.

cyberbezpieczeństwu we wszystkich dziedzinach gospodarki oraz optymalnie wykorzystać dostępną w Europie wiedzę.

23 W tym obszarze postanowiono wesprzeć zaawansowane umiejętności cyfrowe, zwłaszcza w dziedzinie obliczeń wielkiej skali, sztuczną inteligencję, rozproszone rejestry, np. technologie blockchain oraz cyberbezpieczeństwo. Wskazano, że w tym zakresie mają być zrealizowane długoterminowe szkolenia i kursy dla studentów, informatyków i innych pracowników.

24 Według założeń powinna być zapewniona możliwość wprowadzenia i wykorzystania nowoczesnych technologii cyfrowych w sektorze publicznym w takich dziedzinach, jak: ochrona zdrowia, opieka, edukacja, transport, a także kultura oraz sektor kreatywny. Przewidziano, że administracja publiczna oraz przemysł, zwłaszcza małe i średnie przedsiębiorstwa, powinny uzyskać wsparcie we wprowadzeniu technologii cyfrowej.

Ponieważ cyfryzacja dotyczy wszystkich dziedzin życia i wszystkich ludzi, więc niezwykle ważne jest, żeby wszyscy obywatele Unii mogli z niej czerpać korzyści. Cyfryzacja w Europie musi się dokonywać w sposób integrujący. Nikt nie może być wykluczany z dostępu do rozwoju cyfrowego z racji płci, statusu społecznego, poziomu wykształcenia, kwalifikacji, umiejętności cyfrowych, pochodzenia, wieku czy niepełnosprawności. Co ciekawe, nie wskazano tu takich kwestii jak: narodowość, język, religia, poglądy społeczne i polityczne oraz względy rasowe. W opinii podniesiono, że cyfrowy zysk musi zostać sprawiedliwie rozdzielony przez odpowiednie działania polityczne i nie może zapewniać korzyści tylko kilku zainteresowanym grupom. Trzeba mieć przy tym na uwadze zasadę, że jednostka powinna pozostać właścicielem swoich danych.

W opinii wywiedziono, że Europejski Komitet chciałby ściśle powiązać program z realiami społecznymi. Dostrzeżono możliwe skutki cyfryzacji dla rynku pracy oraz zróżnicowane jej oddziaływanie na poszczególne regiony. Wyrażono pragnienie, żeby Unia była postrzegana na światowym rynku jako podmiot szerzący wiedzę, który jest w stanie dotrzymać kroku konkurentom takim, jak Chiny i Stany Zjednoczone Ameryki. Zauważono, że program „Cyfrowa Europa" może wiele zdziałać na polu zwalczania cyberprzestępczości oraz w opracowywaniu sposobów i strategii walki z atakami cybernetycznymi poza Europą. Jednocześnie wskazano na konieczność stworzenia niezależnego europejskiego przemysłu mikroprocesorów.

W opinii opowiedziano się za tym, żeby podczas wszelkich działań w ramach programu brać pod uwagę zasady etyczne. Przypomniano, że Europejski Komitet postuluje urzeczywistnić zasadę kontrolowania maszyny przez człowieka, zwłaszcza w zakresie użytkowania sztucznej inteligencji w środowisku pracy. Wskazano, że trzeba zadbać o to, żeby powstały akty normatywne dotyczące odpowiedzialności prawnej, ochrony danych, ochrony pracowników oraz ochrony konsumentów. Zauważono, że cyfryzacja społeczeństwa Europy powiedzie się tylko wtedy, kiedy oprócz aktów normatywnych uruchomi się transformację kulturalną, która będzie zwiększać świadomość korzyści i zagrożeń związanych z przemianami cyfrowymi.

W opinii skonstatowano, że cyfryzacja i transformacje w środowisku pracy i życia przychodzą wraz z postępem technologicznym i są wszechobecne. Z zadowoleniem przyjęto opracowanie przez Komisję Europejską programu „Cyfrowa Europa". Wskazano, że wyznaczenie w nim priorytetów może przynieść wymierne korzyści dzięki wspieraniu nowoczesnej technologii. W ocenie Europejskiego Komitetu pomoże to uporać się z najtrudniejszymi problemami współczesnego społeczeństwa, będzie korzystne dla tworzenia miejsc pracy

i konkurencyjności, a także poprawi ogólny standard życia wszystkich obywateli[25]. Komitet zwrócił uwagę na konieczność inwestycji społecznych w związku z transformacją cyfrową tak, żeby mogło z niej korzystać całe społeczeństwo. Po raz kolejny zwrócono uwagę, że człowiek musi zachować kontrolę nad maszyną, zwłaszcza w dziedzinie sztucznej inteligencji.

Wyrażono zadowolenie, że Komisja Europejska programem „Cyfrowa Europa" wspiera wprowadzenie i optymalne wykorzystanie zdolności cyfrowych. Zgodzono się z Komisją, że zdolności cyfrowe tworzą podstawę innowacji w obszarach interesu publicznego i działalności gospodarczej. Za ważne uznano zrobienie wszystkiego, żeby całe społeczeństwo europejskie mogło uczestniczyć w rozwoju technicznym. Zdaniem Europejskiego Komitetu program „Cyfrowa Europa" powinien postawić sobie za cel sprawiedliwe rozdzielenie na całą ludność Europy cyfrowego zysku. Podkreślono, że konieczne jest zbudowanie niezależnego europejskiego przemysłu mikroprocesorowego poprzez program wsparcia obliczeń wielkiej skali[26]. Za ważne uznano wspólne opracowanie metod i strategii przeciwdziałania cyberatakom z zewnątrz[27], a także stworzenie norm dotyczących jednolitego rynku cyfrowego i konsekwentne stosowanie europejskiego ogólnego rozporządzenia o ochronie danych i jego udoskonalenie, w szczególności do zastosowania sztucznej inteligencji[28]. Odniesiono się także do kwestii autonomicznego kierowania pojazdami[29]. W opinii podkreślono, że kierowanie się wartościami europejskimi (ochrona danych, ochrona prywatności, ochrona socjalna, zrównoważony rozwój) w rozwoju sztucznej inteligencji mogłoby stanowić przewagę konkurencyjną, gdy ludzie będą coraz bardziej uwrażliwieni na metody wykorzystywania danych przez strony trzecie, np. Stany Zjednoczone, i na potencjał monitorowania, np. Chiny. Europejski Komitet uznał za szczególnie korzystne to, że w programie „Cyfrowa Europa" w kilku miejscach cyfryzacja przemysłu została wysunięta na pierwszy plan, podniósł jednak, że transformacja cyfrowa uda się tylko wówczas, gdy wszystkie przedsiębiorstwa i ich pracownicy będą czerpać z tego korzyści.

25 Wskazano, że znajduje to potwierdzenie w tym, że Komisja Europejska w komunikacie w sprawie wieloletniego planu finansowego przedstawia scenariusz podwojenia inwestycji w cyfryzację. Zob. COM (2018) 98 final.
26 Zob. Dz. Urz. UE 2018, C 283, s. 89.
27 Ibidem, C 227, s. 86.
28 Ibidem 2017, C 288, s. 1; 2018, C 440, s. 51; 2018, C 440, s. 183.
29 Ibidem. s. 8.

W opinii Komitet wskazał konieczność ścisłego powiązania wsparcia wynikającego z programu „Cyfrowa Europa" z programem „Horyzont 2020" („Horyzont Europa"), które oparte są na postępowaniu zgodnym z Europejską Kartą Naukowca[30] oraz na zasadach odpowiedzialnych badań naukowych oraz innowacji[31] i tzw. otwartej nauki[32].

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Skoordynowany plan w sprawie sztucznej inteligencji"

W dniu 7 grudnia 2018 roku został opublikowany Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Skoordynowany plan w sprawie sztucznej inteligencji"[33]. W treści tego dokumentu przypominiano wcześniejszą definicję sztucznej inteligencji oraz stwierdzono, że zmiany związane ze sztuczną inteligencją rodzą nadzieje, ale i budzą obawy, ponieważ pracownicy lękają się utraty pracy z powodu automatyzacji, konsumenci zastanawiają się, kto będzie odpowiedzialny za złą decyzję podjętą przez system oparty na sztucznej inteligencji, małe przedsiębiorstwa nie wiedzą jak zastosować sztuczną inteligencję w swojej działalności gospodarczej, a przedsiębiorstwa typu start-up mogą nie znaleźć w Europie potrzebnych im zasobów i wykwalifikowanych pracowników. Przypomniano, że opublikowana przez Komisję w kwietniu 2018 roku strategia europejska zachęca do wykorzystywania sztucznej inteligencji do rozwiązywania problemów dotyczących leczenia chorób, przeciwdziałania zmianom klimatu, przewidywania klęsk żywiołowych, zwiększenia bezpieczeństwa transportu, a także do walki z przestępczością i poprawy cyberbezpieczeństwa. Zauważono ponadto, że strategia wspiera tworzenie w Europie etycznych, bezpiecznych i najnowocześniejszych rozwiązań

30 https://euraxess.ec.europa.eu/jobs/charter [dostęp: 20.09.2022].

31 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society [dostęp: 24.09.2022].

32 https://ec.europa.eu/research/openscience/ [dostęp: 20.09.2022].

33 Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Skoordynowany plan w sprawie sztucznej inteligencji", Bruksela, 7 grudnia 2018 r., COM (2018) 795 final.

w dziedzinie sztucznej inteligencji. Wykorzystuje też mocne strony Europy w nauce i przemyśle, opierając się na trzech filarach: zwiększenie inwestycji publicznych i prywatnych w sztuczną inteligencję, przygotowanie się na zmiany społeczno-gospodarcze oraz zapewnienie odpowiednich uregulowań etycznych i prawnych.

W swojej strategii w sprawie sztucznej inteligencji dla Europy Komisja zaproponowała opracowanie planu, którego celem jest maksymalizacja wpływu inwestycji na poziomie unijnym i krajowym, wspieranie synergii i współpracy w całej Unii Europejskiej oraz wspólne określenie dalszych działań w celu zapewnienia takich warunków, żeby Unia jako całość mogła sprostać światowej konkurencji. Wniosek skoordynowanego planu opracowano na podstawie deklaracji o współpracy w dziedzinie sztucznej inteligencji przyjętej w kwietniu 2018 roku podczas Dnia Technologii Cyfrowych i podpisanej przez wszystkie państwa członkowskie oraz Norwegię[34]. W czerwcu 2018 roku plan zatwierdziła Rada Europejska[35].

Państwa członkowskie Grupy ds. Cyfryzacji Europejskiego Przemysłu i Sztucznej Inteligencji, a także Norwegia, Szwajcaria i Komisja opracowały plan działań podczas posiedzeń od czerwca do listopada 2018 roku. Rozmowy prowadzono także podczas posiedzeń Rady ds. Konkurencyjności w trakcie austriackiej prezydencji w Radzie UE. Rezultatem tych działań był skoordynowany plan, którego tekst został włączony do komunikatu Komisji z 7 grudnia 2018 roku. Zawiera on szczegółowy opis przedsięwzięć na lata 2018–2020 i przygotowuje pole do działań w kolejnych latach. Plan ten, zgodnie z założeniem, miał być co roku poddawany przeglądowi i aktualizacji.

Zobowiązano wszystkie państwa członkowskie do opracowania krajowych strategii w dziedzinie sztucznej inteligencji do połowy 2019 roku, na podstawie prac prowadzonych na poziomie europejskim. Wspomniane strategie powinny określać poziomy inwestycji i środki wykonawcze[36]. Komisja zaproponowała,

34 https://ec.europa.eu/digital-single-market/en/news/eu-member-sign-cooperate-artificial-intelligence [dostęp: 12.10.2022].

35 https://www.consilium.europa.eu/pl/press/press-releases/2018/06/29/20180628-euco-conclusions-final/ [dostęp: 12.10.2022].

36 Francja, Finlandia, Szwecja, Zjednoczone Królestwo i Niemcy w momencie wydawania komunikatu dysponowały już strategiami dotyczącymi sztucznej inteligencji. Dania, Luksemburg, Niderlandy, Irlandia i Norwegia wprowadziły działania związane ze sztuczną inteligencją do swoich strategii odnoszących się do cyfryzacji. Austria, Belgia, Czechy, Estonia, Włochy, Łotwa, Polska, Portugalia, Słowenia, Słowacja i Hiszpania w momencie publikowania komunikatu Komisji były w trakcie opracowywania takich strategii. Pozostałe państwa unijne i Szwajcaria nie rozpoczęły jeszcze w tym momencie takich działań.

żeby w okresie programowania, tj. od 2021 do 2027 roku, Unia inwestowała w sztuczną inteligencję co najmniej 1 mld euro rocznie z programów „Horyzont Europa" i „Cyfrowa Europa". W treści komunikatu zaproponowano stworzenie warunków do nowego partnerstwa na rzecz badań naukowych i innowacji w dziedzinie sztucznej inteligencji oraz zwiększenie w Europie współpracy między środowiskiem naukowym a przemysłem. Wskazano jednocześnie konieczność utworzenia Europejskiej Rady ds. Innowacji, której celem powinno być wsparcie najnowocześniejszych technologii i najbardziej innowacyjnych przedsiębiorstw typu start-up. Zwrócono uwagę na konieczność wspierania godnych zaufania technologii sztucznej inteligencji i ich rozpowszechniania[37]. Stwierdzono, że istnieje potrzeba dostosowania programów i systemów nauczania oraz szkoleń w celu lepszego przygotowania społeczeństwa europejskiego na sztuczną inteligencję. Podniesiono konieczność rozwijania europejskiej przestrzeni danych mającej ważne znaczenie dla rozwoju sztucznej inteligencji[38]. Zwrócono uwagę na potrzebę opracowania wytycznych dotyczących etyki i zapewnienia podstaw prawnych sprzyjających innowacjom. Przypomniano, że Komisja powierzyła niezależnej grupie ekspertów wysokiego szczebla ds. sztucznej inteligencji zadanie przygotowania projektu wytycznych dotyczących etyki związanej ze sztuczną inteligencją. Podkreślono, że pierwsza wersja tego dokumentu powinna zostać opublikowana pod koniec 2018 roku, a w marcu następnego roku po przeprowadzeniu powszechnej konsultacji za pośrednictwem europejskiego sojuszu na rzecz sztucznej inteligencji eksperci przedstawią Komisji ostateczną wersję wytycznych. Celem tych działań ma być wprowadzenie europejskiego podejścia do etyki na fora międzynarodowe oraz otwarcie współpracy z państwami niebędącymi członkami Unii, które chcą dzielić z Unią te same wartości[39]. W komunikacie podkreślono, że dalszy rozwój sztucznej inteligencji wymaga rozwiązań elastycznych, żeby wspierać innowacje, ale jednocześnie zapewnić wysoki poziom ochrony i bezpieczeństwa. Zadeklarowano, że Komisja opublikuje do połowy 2019 roku sprawozdanie dotyczące ewentualnych luk w normach prawnych dotyczących bezpieczeństwa i odpowiedzialności w odniesieniu do sztucznej inteligencji

37 Szczegółowe informacje na ten temat zostały określone w sekcji C „Skoordynowanego planu…".

38 Wskazano, że szczególnie obiecujące jest zastosowanie sztucznej inteligencji w dziedzinie opieki zdrowotnej. Zadeklarowano, że w 2020 r. Komisja, we współpracy z państwami członkowskimi, wesprze za pośrednictwem programu „Horyzont 2020" rozwój wspólnej bazy danych obrazów zdrowotnych.

39 https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance [dostęp: 12.10.2022].

oraz kierunków rozwoju tych norm. Podniesiono także problem zastosowania sztucznej inteligencji w systemach uzbrojenia.

W załączniku do komunikatu Komisji z 7 grudnia 2008 roku „Skoordynowany plan w sprawie sztucznej inteligencji" na wielu stronach określono działania strategiczne, zasady maksymalizacji inwestycji, problemy dotyczące nauki i zdobywania umiejętności oraz odnoszące się do tworzenia wspólnej europejskiej przestrzeni danych, kwestie etyczne, zagadnienie stosowania sztucznej inteligencji w sektorze publicznym, a także odniesiono się do problemów współpracy międzynarodowej.

Opinia Europejskiego Komitet Ekonomiczno-Społecznego o „Skoordynowanym planie w sprawie sztucznej inteligencji"

Europejski Komitet Ekonomiczno-Społeczny, opiniując „Skoordynowany plan w sprawie sztucznej inteligencji", poparł inicjatywę przeznaczenia większych środków na innowacje, infrastrukturę, edukację i szkolenia związane ze sztuczną inteligencją poprzez instrumenty finansowe Unii. Wezwał jednocześnie państwa członkowskie do podjęcia niezbędnych kroków do osiągnięcia celów określonych w „Skoordynowanym planie…"[40]. W treści opinii wskazano, że proponuje się w nim wspólne działania w czterech obszarach, a mianowicie: zwiększania inwestycji, zwiększania dostępności danych, wspierania talentów i umiejętności oraz zapewnianie zaufania. Dodano, że wezwano państwa członkowskie do opracowania krajowych strategii dotyczących sztucznej inteligencji do połowy 2019 roku. W dalszej części opinii podkreślono, że Europejski Komitet z zadowoleniem przyjął „Skoordynowany plan..." jako ważny krok w kierunku poprawy wdrażania strategii. Przypomniano, że w swojej poprzedniej opinii Komitet przedstawił uwagi dotyczące tej strategii[41]. Nawiązano

40 Opinia Europejskiego Komitetu Ekonomiczno-Społecznego, Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Skoordynowany plan w sprawie sztucznej inteligencji", Dz. Urz. UE 2019, C 240, s. 51. Opinia została przyjęta przez Sekcję Jednolitego Rynku, Produkcji i Konsumpcji 2 kwietnia 2019 r., a 15 maja tegoż roku na sesji plenarnej nr 543 większością 210 głosów „za", przy dwóch głosach „przeciw" i jednym wstrzymującym się. Sprawozdawczynią była Tellervo Kylä-Harakka-Ruonala.

41 Dz. Urz. UE 2018, C 440, s. 51.

także do opinii Europejskiego Komitetu w sprawie programu „Cyfrowa Europa"[42] oraz do opinii przygotowanych przez Europejski Komitet z własnej inicjatywy w sprawie różnych aspektów sztucznej inteligencji[43]. W opinii wskazano, że ważne jest to, żeby środki wykonawcze były planowane na szczeblu zarówno Unii Europejskiej, jak i państw członkowskich, gdyż trzeba pamiętać, że kompetencje Unii i państw członkowskich różnią się w poszczególnych obszarach polityki. Ponadto stwierdzono, że oprócz współpracy i koordynacji między decydentami politycznymi na różnych szczeblach konieczna jest również współpraca między wszystkimi podmiotami społeczeństwa. W treści opinii wezwano do pilnego wdrożenia strategii, gdyż postępy w opracowaniu i wprowadzaniu sztucznej inteligencji poza Unią przebiegają bardzo szybko. Podkreślono, że Unia i państwa członkowskie powinny ściśle trzymać się długoterminowych celów strategii.

Zaproponowano, żeby Unia przyjęła zasady zrównoważonego rozwoju jako podejście przewodnie dla przyszłego rozwoju sztucznej inteligencji. Zauważono przy tym, że zrównoważony rozwój z jego trzema wymiarami wymaga polityki i środków, które wzmacniają gospodarkę i tworzą dobrobyt społeczeństwa, a jednocześnie przyczyniają się do zmniejszenia wpływu na klimat i środowisko. Strategie związane ze sztuczną inteligencją muszą być opracowywane z punktu widzenia podmiotów społeczeństwa obywatelskiego, w tym przedsiębiorstw, pracowników i konsumentów. Za konieczne uznano zminimalizowanie zagrożeń, jakie sztuczna inteligencja może rodzić dla procesów demokratycznych, umożliwiając manipulowanie tymi procesami. Podkreślono znaczenie „niepozostawiania nikogo w tyle" w rozwoju i wprowadzaniu sztucznej inteligencji. Unia powinna w pełni wykorzystać sztuczną inteligencję w analizie prognostycznej w sektorach takich, jak: opieka zdrowotna, transport oraz praca.

42 Ibidem 2019, C 62, s. 292. Opinia ta została wydana już po opublikowaniu komunikatu Komisji „Skoordynowany plan…" 7 grudnia 2018 r.

43 Ibidem 2017, C 288, s. 43; C 345, s. 52; 2018, C 440, s. 1; 2019, C 190, s. 17. Analiza wskazanych dokumentów dowodzi, że w Dz. Urz. UE 2017, C 288, s. 43 znajduje się opinia Komitetu Ekonomiczno-Społecznego przyjęta na sesji plenarnej 31 maja 2017 r. i dotycząca czterech różnych aspektów odnoszących się do trzech dyrektyw Parlamentu Europejskiego i Rady oraz jednego rozporządzenia Parlamentu Europejskiego i Rady, ale żadna z tych kwestii nie dotyczy bezpośrednio problematyki sztucznej inteligencji. Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wpływ cyfryzacji i robotyzacji transportu na kształtowanie polityki UE" (Dz. Urz. UE 2017, C 345, s. 52) odnosi się do ważnych kwestii automatyzacji, robotyzacji i cyfryzacji transportu, nie dotyka zaś problematyki sztucznej inteligencji.

Wskazano, że w Unii dochodzi do wielu wydarzeń związanych z rozwojem i wprowadzaniem sztucznej inteligencji, dlatego podkreślono, że powinna ona zwiększyć wysiłki na rzecz poprawy swojej konkurencyjności poprzez koncentrację na inwestycjach w innowacje i infrastrukturę oraz dalszy rozwój jednolitego rynku. Podkreślono, że Europejski Komitet popiera inicjatywy zmierzające do przeznaczenia większych środków na rozwój i wprowadzanie sztucznej inteligencji. Wskazano, że takie instrumenty, jak: „Horyzont Europa", „Cyfrowa Europa", „InvestEU" i Europejski Fundusz na rzecz Inwestycji Strategicznych, są cenne i niezbędne, dlatego że służą pobudzaniu innowacji w dziedzinie sztucznej inteligencji i inwestycji w nią. Zadeklarowano poparcie planów Komisji dotyczących zacieśnienia współpracy transgranicznej, partnerstw i sieci za pomocą powiązanych ze sobą centrów doskonałości badawczej, ośrodków badawczych i centrów innowacji cyfrowych. Wezwano do zwiększenia inwestycji w technologię i infrastrukturę wymaganą przez sztuczną inteligencję oraz aplikacje wykorzystujące sztuczną inteligencję.

Konstatując, jako że sztuczna inteligencja opiera się głównie na danych, dlatego Europejski Komitet uznał, że ważne znaczenie ma zapewnienie jakości, dostępności, interoperacyjności i sprawnego przepływu danych z jednoczesnym zagwarantowaniem ich ochrony i prywatności. Europejski Komitet poparł w opinii inicjatywy Komisji dotyczące utworzenia wspólnej europejskiej przestrzeni danych. Wezwał do stworzenia warunków sprzyjających tworzeniu europejskich płaszczyzn wymiany danych, a także programów wspierających innowacje. W dalszej części wezwano decydentów politycznych do rozważenia instrumentów politycznych ważnych z punktu widzenia sztucznej inteligencji.

Ponieważ ludzie nie są w dostatecznym stopniu świadomi możliwości, jakie daje im sztuczna inteligencja, przy czym wyraźne są obawy dotyczące kontroli nad maszyną, więc istnieje potrzeba zwiększenia świadomości korzyści, jakie sztuczna inteligencja stwarza dla ogółu społeczeństwa. Wezwano państwa członkowskie do reagowania na nowe zapotrzebowania i umiejętności w warunkach sztucznej inteligencji. Za potrzebne uznano reformy programów nauczania od szkół podstawowych po uniwersytety, szczególnie nauk ścisłych, technologii, inżynierii i matematyki. Powinno się zapewnić obywatelom możliwość przekwalifikowania się, przy czym regułą powinno być uczenie się przez całe życie i kształcenie ustawiczne.

Za konieczne uznano zwiększenie zaufania do sztucznej inteligencji. W tym kontekście poparto wytyczne dotyczące etyki opracowane przez europejską grupę ekspertów wysokiego szczebla. Stwierdzono, że obawy związane ze sztuczną inteligencją przypuszczalnie zmniejszą się wraz z rosnącą wiedzą o niej,

o sposobach jej wykorzystania oraz o zasadach podejmowanych przez nią decyzji. W opinii podkreślono, że stworzy to podstawy zaufania do sztucznej inteligencji przez umożliwienie krytycznego myślenia i uwzględnienia zasadniczych kwestii takich jak problem „zachowania kontroli przez człowieka". Podkreślono, że zaufanie zależy także od takich praktycznych aspektów jak przyjazność dla użytkownika. W dalszej części opinii Komitet zaaprobował opracowane przez europejską grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji wytyczne w dziedzinie etyki dotyczące zaufania do sztucznej inteligencji. Podkreślił, że kluczowe znaczenie mają otwarte, odpowiednie i wiarygodne dane oraz przejrzystość decyzji. Wezwał do powszechnych dyskusji o skutkach profilowania ludzi i niezbędnych warunków do kwestionowania decyzji w sprawie sztucznej inteligencji.

Komitet zwrócił uwagę na konieczność rozważania kwestii etycznych w zrównoważonym rozwoju, ponieważ obejmują one głównie aspekty związane z działalnością człowieka i w tej sytuacji wchodzą w zakres społecznego wymiaru zrównoważonego rozwoju. Zwrócił uwagę, że sztuczna inteligencja powinna uwzględniać aspekty środowiskowe związane ze zmianą klimatu i zasobami naturalnymi, w tym zrównoważone wykorzystanie energii i surowców oraz unikanie sztucznego skracania cyklu życia produktów. Zauważył, że zrównoważony rozwój wymaga, żeby rozwiązania w dziedzinie sztucznej inteligencji były racjonalne z ekonomicznego punktu widzenia, tj. wydajne, rentowne i konkurencyjne. Podkreślił, że sztuczna inteligencja winna przynosić korzyści społeczeństwu w duchu zrównoważonego rozwoju, przyczyniać się do dobrobytu gospodarczego, społecznego oraz do dobrostanu w dziedzinie zdrowia. Zwrócił uwagę na wpływ sztucznej inteligencji na ochronę środowiska.

Europejski Komitet podniósł, że można zwiększyć zaufanie do sztucznej inteligencji dzięki polityce publicznej skoncentrowanej na obywatelu i poprzez zaangażowanie przedstawicieli społeczeństwa obywatelskiego w opracowywanie strategii politycznych i środków związanych ze sztuczną inteligencją. Cel taki może sektor publiczny osiągnąć poprzez zorientowaną na obywatela administrację, w której sztuczna inteligencja mogłaby odegrać znaczącą rolę dzięki usprawnieniu i lepszemu dostosowaniu procesów administracyjnych. Zwrócił uwagę, że rozwój sztucznej inteligencji musi odbywać się w pełnej zgodności z prawem, niezależnie od tego, czy chodzi o przepisy dotyczące konsumentów, pracowników czy przedsiębiorstw. Konstatując istnienie wielkiej liczby przepisów mających znaczenie dla rozwoju i stosowania sztucznej inteligencji, Europejski Komitet wezwał Komisję do sfinalizowania oceny odpowiednich aktów normatywnych dotyczących bezpieczeństwa i odpowiedzialności pod kątem ich przydatności w odniesieniu do sztucznej inteligencji.

Komitet uznał, że najważniejszą rzeczą jest to, żeby zasady wiarygodnych systemów sztucznej inteligencji były przyjmowane i wprowadzane jako integralna część kultury każdej organizacji zarówno w sektorze prywatnym, jak i publicznym. Wskazał, że etyka sztucznej inteligencji ma być postrzegana jako odrębna lub różna od ogólnych zasad etyki. Kwestie etyki sztucznej inteligencji powinny być uwzględnione w ogólnych strategiach, w kodeksach etycznych i regularnych praktykach zarządzania. Podkreślił, że proaktywne przyjęcie wiarygodnych systemów sztucznej inteligencji można wzmocnić przez włączenie aspektów etycznych do programów kształcenia twórców i użytkowników sztucznej inteligencji. Zadeklarował, że Europejski Komitet jest gotów ze swej strony rozpowszechniać informacje dotyczące aspektów etycznych wśród podmiotów społeczeństwa obywatelskiego.

Komunikat Komisji „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka" z 8 kwietnia 2019 roku

W komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka" z 8 kwietnia 2019 roku[44] wskazano korzyści, jakie sztuczna inteligencja niesie ze sobą. Wspomniano, że jest to technologia strategiczna, która obecnie rozwija się i jest wykorzystywana w szybkim tempie na całym świecie. Niesie ona ze sobą nowe wyzwania dla przyszłości pracy, ale rodzi także wątpliwości natury prawnej i etycznej. Przypomniano, że w celu przezwyciężenia tych problemów i w jak największym stopniu wykorzystania możliwości sztucznej inteligencji Komisja opublikowała strategię europejską, która stawia w centrum rozwoju człowieka – „sztuczna inteligencja ukierunkowana na człowieka". Uznano, że jest to trójpłaszczyznowe podejście do zwiększenia zdolności technologicznych i przemysłowych Unii Europejskiej oraz wykorzystania sztucznej inteligencji w całej gospodarce, a także przygotowania się do zmian społeczno-gospodarczych oraz zapewnienia odpowiednich norm etycznych i prawnych. Jeżeli chodzi o działania dotyczących strategii na rzecz sztucznej inteligencji, to Komisja wraz z państwami członkowskimi wypracowała skoordynowany plan

44 COM(2019) 168 final, Bruksela 8 kwietnia 2019 r.

w dziedzinie sztucznej inteligencji, który to plan przedstawiła w grudniu 2018 roku[45]. Jego celem było stworzenie synergii, zebranie danych oraz zwiększenie wspólnych inwestycji. Chodziło przy tym o wzmocnienie współpracy transgranicznej oraz mobilizację wszystkich zainteresowanych podmiotów w celu zwiększenia inwestycji publicznych i prywatnych[46]. Przypomniano, że europejska strategia sztucznej inteligencji oraz skoordynowany plan jasno wskazują, że zaufanie jest warunkiem wstępnym do zapewnienia podejścia do sztucznej inteligencji ukierunkowanego na człowieka. Podkreślono, że sztuczna inteligencja nie jest celem samym w sobie, ale narzędziem, które musi służyć ludziom do zwiększenia ich dobrostanu, dlatego trzeba zadbać o wiarygodność sztucznej inteligencji. Przypomniano, że podstawą działania Unii są wartości takie, jak: poszanowanie godności osoby ludzkiej, wolność, demokracja, równość, praworządność, poszanowanie praw człowieka, w tym praw osób należących do mniejszości. Wartości te są wspólne dla społeczeństw wszystkich państw członkowskich, w których panuje pluralizm, niedyskryminacja, tolerancja, sprawiedliwość, solidarność i równość. Wskazano, że Karta praw podstawowych Unii Europejskiej ujmuje w jednym tekście wszystkie prawa jednostki, prawa obywatelskie, polityczne, gospodarze i społeczne, z których korzystają mieszkańcy Unii. Unia dysponuje mocnymi filarami prawnymi określającymi globalny standard w odniesieniu do sztucznej inteligencji ukierunkowanej na człowieka. Przypomniano, że przyjęty niedawno akt w sprawie cyberbezpieczeństwa przyczynił się do wzmocnienia zaufania do internetu, a przygotowywane rozporządzenie w sprawie prywatności i łączności elektronicznej[47] zmierza do tego celu. Przypomniano, że technologia sztucznej inteligencji powinna być rozwijana w sposób, który stawia człowieka w centrum, a zastosowania sztucznej inteligencji powinny być zgodne nie tylko z prawem, lecz także z zasadami etycznymi. Podkreślono, że na każdym etapie rozwoju sztucznej inteligencji należy zapewnić różnorodność pod względem płci, pochodzenia rasowego lub etnicznego, religii lub przekonań, niepełnosprawności i wieku. Zauważono, że istnieje potrzeba opracowania wytycznych dotyczących etyki na podstawie istniejących norm prawnych. Zasady te powinny być jednakowe we wszystkich państwach członkowskich.

45 COM (2018) 795.

46 Komisja podwoiła swoje inwestycje w sztuczną inteligencję w ramach programu „Horyzont 2020", planuje inwestować dalsze środki corocznie z programów „Horyzont Europa" oraz „Cyfrowa Europa".

47 COM (2017) 10.

Przypomniano, że z tego właśnie względu Komisja utworzyła grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji[48], która opracowała wytyczne odnośnie do etyki oraz przygotowała katalog zaleceń dotyczących powszechnej polityki w dziedzinie sztucznej inteligencji. Jednocześnie utworzono Europejski Sojusz na Rzecz Sztucznej Inteligencji[49]. Wspomniana grupa ekspertów wysokiego szczebla opublikowała pierwszy projekt wytycznych dotyczących etyki, który to projekt po spotkaniach i konsultacjach został poprawiony i opublikowany w marcu 2019 roku.

We wspomnianych wytycznych stwierdzono, że do osiągnięcia „wiarygodnej sztucznej inteligencję" konieczne jest zachowanie i zaistnienie trzech elementów. Po pierwsze, powinna być ona zgodna z przepisami prawa, po drugie rozwijana z poszanowaniem zasad etycznych, po trzecie ma być solidna. Na tej podstawie określono siedem najważniejszych wymogów, które powinny być spełnione, żeby sztuczną inteligencję można uznać za wiarygodną. Wśród tych wymogów wskazano: przewodnią i nadzorczą rolę człowieka; techniczną solidność i bezpieczeństwo; ochronę prywatności i danych; przejrzystość; różnorodność, niedyskryminację i sprawiedliwość; dobrostan społeczny i środowiskowy; odpowiedzialność. Wskazano, że nie mają one charakteru wiążącego, ponieważ jako takie nie tworzą żadnych nowych zobowiązań prawnych, ale osiągnięcie porozumienia w sprawie kluczowych wymogów wobec systemu sztucznej inteligencji jest pierwszym, ważnym krokiem w kierunku wypracowania wytycznych dotyczących etycznej sztucznej inteligencji. W dalszej części dokumentu przedstawiono plan, według którego będą przebiegały prace. Przewidziano, że na początku 2020 roku zostanie dokonany przegląd i aktualizacja wytycznych, a Komisja oceni wyniki i zaproponuje dalsze działania.

Opinia Europejskiego Komitet Ekonomiczno-Społecznego w sprawie komunikatu Komisji „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka"

Europejski Komitet Ekonomiczno-Społeczny, opiniując komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu

48 *High-level expert group on artificial intelligence*, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence [dostęp: 14.10.2022].
49 *The European AI Alliance*, https://ec.europa.eu/digital-single-market/en/european-ai-alliance [dostęp: 14.10.2022].

Ekonomiczno-Społecznego i Komitetu Regionów „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka”[50], przypomniał, że powstał on na podstawie prac grupy ekspertów wysokiego szczebla, którą Komisja utworzyła w czerwcu 2018 roku. Zwrócono uwagę, że Komisja, powołując ekspertów, określiła siedem wymogów, którym powinien odpowiadać ostateczny projekt. Komisja rozpoczęła także fazę pilotażową z udziałem wielu zainteresowanych stron. W jej trakcie skoncentrowano się na liście kontrolnej, którą grupa ekspertów wysokiego szczebla sporządziła w odniesieniu do każdego z kluczowych wymogów. Podkreślono, że na początku 2020 roku wspomniana grupa dokona przeglądu i aktualizacji listy kontrolnej, a Komisja zaproponuje w razie konieczności nowe środki.

Wywiedziono, że sztuczna inteligencja nie jest celem samym w sobie, lecz narzędziem, które może spowodować radykalne pozytywne przemiany. Ponieważ jednocześnie niesie ze sobą pewne ryzyko, więc konieczne jest opracowanie zasad korzystania ze sztucznej inteligencji. Formułując wnioski i zalecenia, Europejski Komitet podkreślił, że Komisja powinna przedsięwziąć środki mające na celu przewidywanie niewłaściwego wykorzystywania sztucznej inteligencji oraz uczenia się maszyn. Zauważono, że niewłaściwe wykorzystywanie sztucznej inteligencji powinno być zakazane. Za konieczne uznano uregulowanie wprowadzania na rynek produktów, które mogą zostać wykorzystane w złej intencji. Wskazano, że Komisja powinna propagować rozwój systemów sztucznej inteligencji ukierunkowanych na konkretne zastosowania, które pozwoliłyby przyspieszyć transformację ekologiczną i klimatyczną. Za konieczne uznano określenie wyzwań, które można rozwiązać za pomocą kodeksów etycznych, samoregulacji i dobrowolnych zobowiązań, a które na podstawie środków regulacyjnych i prawnych, uzupełnionych o monitorowanie, a w razie niezastosowania się do wymogów – z wykorzystaniem sankcji. Dodano, że w każdym przypadku systemy sztucznej inteligencji muszą być zgodne z obowiązującym prawodawstwem[51].

50 Dz. Urz. UE 2020, C 47, s. 64. Opinia została przyjęta na 547 sesji plenarnej 30 października 2019 r. większością 198 głosów „za”, przy jednym głosie przeciwnym i czterech wstrzymujących się. Sprawozdawczynią była Franca Salis-Mavinier.

51 W opinii zauważono, że sztuczna inteligencja wymaga podejścia obejmującego zarówno aspekty techniczne, jak i społeczne oraz etyczne. Europejski Komitet z zadowoleniem przyjął chęć opracowania przez Unię ukierunkowanego na człowieka podejścia do sztucznej inteligencji, zgodnego z jej fundamentalnymi wartościami: poszanowaniem godności ludzkiej, wolnością, demokracją, równością i niedyskryminacją, praworządnością i poszanowaniem praw człowieka. Potwierdzono sformułowaną w swojej opinii z inicjatywy

Podniesiono, że Komisja powinna propagować dialog społeczny w celu włączenia pracowników w zastosowanie systemów sztucznej inteligencji. W opinii podkreślono, że godna zaufania sztuczna inteligencja zakłada kontrolę człowieka nad maszyną i informowanie obywateli o zastosowaniu systemów sztucznej inteligencji. Zwrócono uwagę, że systemy te powinny być w miarę możliwości wyjaśniane, a jeżeli okazałoby się to niemożliwe, to należy dostarczać obywatelom i konsumentom informacji o ograniczeniach i zagrożeniach związanych z tymi systemami[52]. Stwierdzono, że niezbędne jest opracowanie przepisów przeciwdziałających „pojawiającym się zagrożeniom"[53]. Europejski Komitet opowiedział się za stworzeniem solidnego systemu certyfikacji opartego na procedurach testowych, które umożliwiałyby przedsiębiorcom potwierdzenie wiarygodności i bezpieczeństwa swoich systemów. Zauważono, że przejrzystość, identyfikowalność i wytłumaczalność procesu podejmowania decyzji na podstawie algorytmu są wyzwaniami technicznymi, które wymagają wsparcia w postaci instrumentów Unii takich jak program „Horyzont Europa". Ochrona prywatności i danych osobowych – zdaniem Europejskiego Komitetu – określi poziom zaufania obywateli i konsumentów do sztucznej inteligencji. Zauważono, że własność danych, ich kontrola i wykorzystanie przez przedsiębiorstwa i organizacje to kwestie, które należy uregulować w szczególności w odniesieniu do internetu rzeczy. Europejski Komitet podniósł, że zachęca Komisję, żeby zważywszy na rozwój technologii, dokonywała regularnego przeglądu ogólnego rozporządzenia o ochronie danych (RODO) i związanych z nim przepisów[54]. Podkreślono ponadto, że Europejski Komitet jest

własnej zatytułowanej „Sztuczna inteligencja: przewidywanie jej wpływu na pracę w celu zapewnienia sprawiedliwej transformacji" (Dz. Urz. UE 2018, C 440, s. 1) potrzebę informowania pracowników i ich przedstawicieli oraz przeprowadzania z nimi konsultacji podczas wprowadzania systemów sztucznej inteligencji mogących zmienić organizację pracy, w tym nadzór i kontrolę, a także systemy oceny i naboru pracowników.

52 Przypomniano tu wcześniejszą opinię wydaną z inicjatywy własnej przez Europejski Komitet Ekonomiczno-Społeczny „Sztuczna inteligencja: wpływ sztucznej inteligencji na jednolity rynek (cyfrowy), produkcję, konsumpcję, zatrudnienie i społeczeństwo" (Dz. Urz. UE 2017, C 288, s. 1) – treść tej opinii omówiono wyżej.

53 *Emerging risks*, https://osha.europa.eu/en/emerging-risks [dostęp: 14.10.2022]. Podkreślono, że niezbędne jest opracowanie przepisów w celu niedopuszczenia do tego, żeby automatyczne systemy przynosiły szkodę lub wyrządzały krzywdę człowiekowi. Uznano, że należy przeszkolić pracowników ze współpracy z maszyną, wskazano, że w nagłych przypadkach istnieje możliwość jej unieruchomienia.

54 Zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz. Urz. UE 2016, L 119, s. 1, z późn. zm.

zdania, że niezbędne jest rozważenie możliwego wkładu systemów sztucznej inteligencji w ograniczanie emisji gazów cieplarnianych, zwłaszcza w sektorach przemysłu, transportu, energii, budownictwa i rolnictwa. Komitet zaapelował, żeby kwestie zmiany klimatu i transformacji cyfrowej były rozważane wspólnie. Podniósł, że kontrola systemów sztucznej inteligencji może być niewystarczająca do określenia zakresu odpowiedzialności i wzbudzenia zaufania. Zalecił nadać priorytet stworzeniu jasnych przepisów, które w przypadku niespełnienia zasad obarczałyby odpowiedzialnością podmioty posiadające osobowość prawną, czyli osoby fizyczne lub prawne. Jednocześnie wezwano Komisję do zbadania w trybie priorytetowym możliwości ubezpieczania systemów sztucznej inteligencji. Zaproponowano opracowanie „europejskiego certyfikatu zaufanego przedsiębiorstwa w sektorze sztucznej inteligencji" na podstawie m.in. listy oceniającej zaproponowanej przez grupę ekspertów wysokiego szczebla do spraw sztucznej inteligencji. Wskazano, że Unia Europejska musi dążyć do tego, żeby uregulowania w sprawie sztucznej inteligencji wykroczyły poza granice europejskie. Uznano, że konieczne jest stworzenie międzynarodowego porozumienia w sprawie godnej zaufania sztucznej inteligencji, które to porozumienie umożliwi opracowanie międzynarodowych norm i regularne sprawdzanie ich adekwatności.

Sztuczna inteligencja ukierunkowana na człowieka wymaga – jak stwierdził w opinii Europejski Komitet – podejścia obejmującego aspekty techniczne, a także społeczne i etyczne. Komitet z zadowoleniem przyjął chęć opracowania przez instytucje Unii podejścia do sztucznej inteligencji zgodnego z leżącymi u jej podstaw wartościami, a mianowicie: poszanowaniem godności ludzkiej, wolnością, demokracją, równością i niedyskryminacją, praworządnością oraz poszanowaniem praw człowieka. W opinii wskazano, że zaufanie do sztucznej inteligencji ukierunkowanej na człowieka narodzi się z potwierdzenia wartości i zasad z jasno określonych aktów prawnych i wytycznych w dziedzinie etyki obejmujących zasadnicze wymogi. Niezbędne jest rozpoznanie wśród licznych wyzwań związanych ze sztuczną inteligencją tych, którym będzie trzeba stawić czoła za pomocą środków regulacyjnych i legislacyjnych połączonych z ustalonymi w przepisach mechanizmami monitorowania oraz ewentualnie sankcjami w razie niestosowania się do wspomnianych środków. Należy ponadto rozpoznać wyzwania, którym będzie można sprostać na podstawie kodeksu etycznego, samoregulacji i dobrowolnych zobowiązań. Europejski Komitet z zadowoleniem zauważył, że Komisja uwzględniła wskazane przez niego zasady, z ubolewaniem jednak stwierdził, że nie zaproponowała na obecnym etapie konkretnych środków mających na celu rozproszenie

uzasadnionych obaw w dziedzinie praw konsumentów, bezpieczeństwa i systemów odpowiedzialności.

W opinii wskazano, że systemy sztucznej inteligencji muszą być zgodne z obowiązującymi aktami prawnymi, w szczególności w odniesieniu do ochrony danych osobowych, odpowiedzialności za produkt, ochrony konsumentów, niedyskryminacji, kwalifikacji zawodowych oraz informowania pracowników i przeprowadzania z nimi konsultacji w miejscu pracy. Dodano, że należy zapewnić dostosowanie tych przepisów do nowych wyzwań związanych z cyfryzacją i sztuczną inteligencją[55]. Przechodząc do uwag szczegółowych, Europejski Komitet stwierdził, że zgadza się z zaproponowanym przez Komisję podejściem do kontroli człowieka nad maszyną oraz ze stanowiskiem, że korzystanie z systemów sztucznej inteligencji w żadnym wypadku nie podważy niezależności ludzkiej ani nie spowoduje negatywnych skutków. Podkreślono, że konieczne jest rzetelne informowanie obywateli o wykorzystaniu systemów sztucznej inteligencji, a tam, gdzie jest to możliwe, żeby ich użytkownicy otrzymywali ostrzeżenia o ograniczeniach i zagrożeniach związanych z systemem.

Szczególną uwagę Europejski Komitet poświęcił ryzyku nadużywania systemów sztucznej inteligencji[56]. W opinii wskazano, że niezbędne jest ustanowienie jasnych przepisów w celu niedopuszczenia do sytuacji, w której współpraca między człowiekiem a maszyną doprowadziłaby do szkód dla ludzi[57]. Komitet podkreślił, że pracownicy powinni zostać przeszkoleni ze stosowania sztucznej inteligencji i robotyki.

55 Europejki Komitet Ekonomiczno-Społeczny wskazał w opinii, że przywiązuje największą wagę do przyszłych metod tej oceny, a także opracowania wskaźników, które mogłyby zostać uwzględnione w celu przeprowadzenia oceny. Projekt listy kontrolnej sporządzonej przez grupę ekspertów wysokiego szczebla jest punktem wyjścia do wdrażania takich procedur. Przy okazji podkreślono, że pozytywne przemiany, które niesie ze sobą sztuczna inteligencja w dziedzinie rozwoju gospodarczego, zrównoważonego charakteru procesów produkcji i konsumpcji (w szczególności energii) oraz poprawy wykorzystania zasobów, powinny być korzystne dla wszystkich państw, a w nich – dla wszystkich obywateli.

56 Dostrzegał je w gromadzeniu bez nadzoru danych osobowych, danych dotyczących zdrowia, w wymianie danych z osobami trzecimi oraz w ryzyku pojawiającym się w dziedzinie bezpieczeństwa i higieny pracy.

57 Podkreślono, że w odniesieniu do robotów współpracujących ustanowiona przez Międzynarodową Organizację Normalizacyjną (ISO) norma dotycząca producentów, podmiotów zajmujących się integracją technologii i użytkowników dostarcza wytycznych w sprawie tworzenia i organizacji przestrzeni roboczej oraz ograniczenia ryzyka, na które mogą zostać narażone poszczególne osoby. Zob. ISO/TS 15066: 2016 Robots and robotic devices – Collaborative robots.

Europejski Komitet opowiedział się za stworzeniem europejskich standardów ochrony oraz solidnego systemu certyfikacji na podstawie procedur badawczych, które umożliwiałyby przedsiębiorcom potwierdzenie wiarygodności używanych systemów sztucznej inteligencji. Podkreślił także znaczenie możliwości ubezpieczenia systemów sztucznej inteligencji, uznał, że kwestia ta powinna być szybko uregulowana.

Z niezadowoleniem odnotowano, że Komisja w niewielkim stopniu porusza kwestię szkodliwego zastosowania sztucznej inteligencji i uczenia się maszyn, mimo że przestrzega przed tym wielu badaczy. Za korzystne uznano uwzględnienie tych zaleceń badaczy, które dotyczą bezpieczeństwa cyfrowego, bezpieczeństwa fizycznego i bezpieczeństwa politycznego[58]. Przy okazji wskazano, że badacze, inżynierowie i organy publiczne muszą ze sobą ściśle współpracować w celu zapobieżenia ryzyku.

Odnosząc się do stanowiska Komisji w sprawie właściwego zarządzania dostępem do danych, Europejski Komitet stwierdził, że czas wyjść poza takie ogólniki. Zauważył, że stopień zaufania obywatela do systemów sztucznej inteligencji będzie decydował o rozwoju tych systemów. Podkreślił, że do uregulowania w dużej mierze pozostają takie kwestie, jak: własność danych, ich kontrola i wykorzystanie przez przedsiębiorstwa i organizacje. Zaznaczono, że budzi wątpliwości np. ilość i rodzaj danych przekazywanych przez samochody ich producentom. Podkreślono, że konsumenci, pomimo zasady uwzględnienia ochrony prywatności, już w fazie projektowania dysponują bardzo ograniczonymi informacjami na temat przekazywania takich danych bądź informacji takich w ogóle nie posiadają i nie ma żadnego sposobu, żeby takie dane kontrolować. Dlatego też Europejski Komitet wezwał Komisję, żeby ze względu na rozwój technologii dokonała przeglądu RODO i związanych z tym rozporządzeniem przepisów.

Zdaniem Europejskiego Komitetu wytłumaczalność procesu podejmowania decyzji na podstawie algorytmu jest niezbędna do zrozumienia mechanizmów jako takich, a także logiki procesów podejmowania decyzji oraz sposobu, w jaki systemy sztucznej inteligencji na nie wpływają. Skonstatowano,

58 Omawiając bezpieczeństwo cyfrowe, wskazano na ataki cybernetyczne, wykorzystanie słabości ludzi i sztucznej inteligencji oraz *data poisoning*. Odnośnie do bezpieczeństwa fizycznego wskazano hakowanie autonomicznych systemów, w tym pojazdów autonomicznych, dronów i broni automatycznej, w kwestii zaś bezpieczeństwa politycznego zwrócono uwagę na masowe gromadzenie danych osobowych, ukierunkowaną propagandę, manipulację wideo itp.

że opracowanie standardowych procedur badawczych dla systemów uczenia maszynowego pozostaje wyzwaniem technicznym i wymaga wsparcia takich instrumentów unijnych, jak program „Horyzont Europa". Europejski Komitet zgodził się ze stanowiskiem Komisji, że systemy sztucznej inteligencji powinny być rozpoznawalne jako takie, zapewniając, że użytkownicy będą świadomi tego, że wchodzą w interakcję z systemem sztucznej inteligencji. Zauważono, że może się to dziać w relacji między pacjentem a pracownikiem służby zdrowia oraz podczas świadczenia profesjonalnych usług związanych ze zdrowiem i dobrostanem obywateli. Podkreślono, że użytkownik lub konsument musi być też informowany o usługach świadczonych przez człowieka. Stwierdzono, że liczne systemy sztucznej inteligencji wymagają *de facto* dużego nakładu pracy ludzkiej, często niewidocznej dla użytkowników. Podkreślono, że wiąże się z tym brak przejrzystości wobec użytkowników i konsumentów usług, a także pewna forma wykorzystania pracy ukrytej i nieuznanej. Zdaniem Europejskiego Komitetu konsument powinien być informowany o systemach sztucznej inteligencji wbudowanych w nabywane produkty i musi mieć nieprzerwanie możliwość dostępu do swoich danych i ich kontroli.

Europejski Komitet stwierdził, że niektóre zastosowania sztucznej inteligencji umożliwiające modelowanie profili obywateli, użytkowników i konsumentów rodzą ryzyko dyskryminacji. Wskazano, że Unia ma wiele przepisów prawnych dotyczących równego traktowania i niedyskryminacji[59]. Systemy sztucznej inteligencji muszą być zgodne z tymi przepisami. Dodano, że do tych przepisów musi się dostosować prawodawstwo regulujące funkcjonowanie sztucznej inteligencji. Skonstatowano, że istnieje rzeczywiste ryzyko, że profilowanie algorytmiczne stanie się nowym potężnym narzędziem dyskryminacji, którego powstaniu Unia musi się przeciwstawić. Wezwano, żeby np. organy powołane do promowania równości kobiet i mężczyzn oraz przeciwdziałania rasizmowi odegrały aktywną rolę w monitorowaniu kontroli systemów sztucznej inteligencji w związku z ryzykiem bezpośredniej lub pośredniej dyskryminacji.

W dalszej części opinii stwierdzono, że Komisja nie przedstawiła konkretnych sposobów połączenia transformacji klimatycznej z transformacją cyfrową, zwłaszcza odnośnie do wykorzystania sztucznej inteligencji. Jednocześnie uznano, że systemy te mogłyby wnieść wkład w ograniczenie emisji gazów cieplarnianych w różnych sektorach. Europejska Komisja skonstatowała, że systemy sztucznej inteligencji można wykorzystać do rozwoju umiejętności

59 Zob. Dz. Urz. UE 2000, L 180, s. 22; L 303, s. 16; 2004, L 373, s. 37; 2006, L 204, s. 23.

społecznych, chociaż mogą się one jednocześnie przyczynić do ich pogorszenia. Zauważono, że Unia musi w większym stopniu uwzględnić niektóre wyzwania społeczne[60]. Podkreślono, że skutki cyfryzacji mogą zaburzać poczucie bezpieczeństwa i wywoływać stres, dlatego też należy opracować strategię antycypowania zmian i kształcenia ustawicznego wszystkich pracowników. Wymaga to wysokiej jakości dialogu między pracodawcami a przedstawicielami pracowników przedsiębiorstwa.

Europejski Komitet stwierdził, że decyzje podejmowane przez systemy uczenia maszynowego nie są łatwe do wyjaśnienia. Podkreślono, że kontrola systemów sztucznej inteligencji może nie wystarczać do określenia zakresu odpowiedzialności i wzbudzenia zaufania. Dlatego też zalecono stworzenie przepisów, które w przypadku niespełnienia zasad obarczałyby odpowiedzialnością podmioty mające osobowość prawną, tj. osoby fizyczne lub prawne. W opinii przypomniano, że w dyrektywie w sprawie odpowiedzialności za produkty[61] ustanowiono zasadę ścisłej odpowiedzialności producentów europejskich. Zdaniem Europejskiego Komitetu wdrażanie i wykorzystywanie systemów sztucznej inteligencji wymaga przyjęcia przez Unię adekwatnych przepisów dotyczących odpowiedzialności w sytuacjach, gdy produkty zawierające treści cyfrowe i związane z nimi usługi mogą się okazać niebezpieczne lub szkodliwe. Konsumenci takiej sytuacji powinni mieć dostęp do wymiaru sprawiedliwości w przypadku szkód spowodowanych przez system sztucznej inteligencji.

Na koniec stwierdzono, że należy kontynuować rozmowy dwustronne w zglobalizowanym świecie tak, żeby większość państw mogła uczestniczyć w procesach normalizacji sztucznej inteligencji i regularnie kontrolować ich stosowność.

60 Wskazano, że projektowanie niektórych aplikacji ma na celu maksymalne wydłużenie korzystania przez użytkowników z usług internetowych, np. z sieci społecznościowych, gier, nagrań wideo. Celem jest umożliwienie gromadzenia maksymalnej ilości danych dotyczących zachowań ludzkich. Wyniki badań wskazują, że efektem jest wzrost poziomu lęku i agresji, brak snu, wpływ na edukację, stosunki społeczne, zdrowie i dobrostan.

61 Dyrektywa Rady z dnia 25 lipca 1985 r. w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących odpowiedzialności za produkty wadliwe, Dz. Urz. UE 1985, L 210, s. 29.

Opinia rozpoznawcza Europejskiego Komitetu Ekonomiczno-Społecznego „Cyfryzacja, sztuczna inteligencja i kapitał własny – jak wzmocnić Unię Europejską w globalnym wyścigu umiejętności i kształcenia przyszłości przy jednoczesnym zapewnieniu włączenia społecznego"

Na sesji plenarnej Europejskiego Komitetu Ekonomiczno-Społecznego 25 września 2019 roku jednogłośnie przyjęto opinię „Cyfryzacja, sztuczna inteligencja i kapitał własny – jak wzmocnić Unię Europejską w globalnym wyścigu umiejętności i kształcenia przyszłości przy jednoczesnym zapewnieniu włączenia społecznego"[62]. Opinia ta, nazywana przez Europejski Komitet opinią rozpoznawczą, była odpowiedzią na pytanie fińskiej prezydencji UE dotyczące sposobów wzmocnienia Unii w globalnym wyścigu umiejętności i kształcenia przyszłości z jednoczesnym zapewnieniem włączenia społecznego w kontekście cyfryzacji i sztucznej inteligencji. Podkreślono, że Europejski Komitet sporządził ostatnio wiele opinii na temat konsekwencji cyfryzacji i sztucznej inteligencji dla przyszłości pracy, zapotrzebowania na umiejętności, potrzeb inwestycyjnych, a także aspektów etycznych związanych ze sztuczną inteligencją[63].

We wstępie do omawianej opinii zwrócono uwagę, że skupia się ona na wzajemnym połączeniu umiejętności cyfrowych i umiejętności związanych ze sztuczną inteligencją, a także konkurencyjności i włączeniu społecznym, bez uwzględniania innych, przyszłych umiejętności, które będą potrzebne do reagowania np. na zmianę klimatu. Wywiedziono, że ze względu na szybki postęp cyfryzacji i sztucznej inteligencji Unia musi się dobrze przygotować do udziału w światowej konkurencji. Skonstatowano, że główną rolę odgrywa tu poprawa umiejętności i kompetencji, a to wymaga aktywnego rozwoju kształcenia i szkolenia, co powinno również wspierać ludzi w zaspokajaniu zmieniających się potrzeb i w kształtowaniu postępu przez śledzenie jego różnych form i skutków. Zauważono, że cyfryzacja i sztuczna inteligencja są na różne sposoby powiązane z rozwojem kształcenia i umiejętności. Generują nowe zapotrzebowania na umiejętności i kompetencje oraz umożliwiają nowe sposoby

62 Ibidem 2020, C 14, s. 46. Sprawozdawczynią była Tellervo Kyllä-Harrakka-Ruonala, a współsprawozdawczynią Giulia Barbucci.

63 Zob. Ibidem 2019, C 240, s. 51; C 228, s. 16; C 62, s. 292; C 218, s. 1; C 110, s. 41; 2018, C 367, s. 15; 2017, C 434, s. 36; C 288, s. 43.

uczenia się i nauczania. Techniki cyfrowe i sztuczną inteligencję można również wykorzystywać do antycypowania zmian w pracy i w życiu codziennym, a tym samym potrzeb w zakresie kształcenia i szkolenia. Ponadto kształcenie i szkolenie umożliwiają ludziom kształtowanie rozwoju cyfrowego. Cyfryzacja i sztuczna inteligencja – jak zauważono w opinii – wiążą się również na wiele sposobów z włączeniem społecznym. Pomagają m.in. osobom niepełnosprawnym pracować i lepiej sobie radzić w życiu. Mogą przyczynić się do zmniejszenia izolacji. Włączenie społeczne wymaga, żeby każdy miał dostęp do tych technologii i niezbędnych umiejętności bez względu na płeć, wiek czy pochodzenie społeczno-ekonomiczne. Wprawdzie, jak zauważono w opinii, ogólnie rzecz biorąc, kształcenie leży w gestii państw członkowskich, ale istnieją różne rodzaje współpracy, jak wymiana dobrych praktyk. Podejmowane są również prace nad stworzeniem europejskiego obszaru edukacji z wykorzystaniem programu Erasmus+ oraz innych instrumentów finansowania istniejących w Unii Europejskiej. Bardzo ważną formą współpracy jest uznawanie kwalifikacji zawodowych. W opinii wskazano, że chcąc rozważyć umiejętności i kształcenie w dziedzinie technologii cyfrowych i sztucznej inteligencji zarówno z punktu widzenia powodzenia w przyszłości światowej konkurencji, jak i włączenia społecznego, Europejski Komitet Ekonomiczno-Społeczny bierze pod uwagę trzy kwestie. Pierwsza z nich sprowadza się do pytania, jakie umiejętności i wiedza są najbardziej istotne w erze sztucznej inteligencji. Druga dotyczy sposobów zdobywania wiedzy i rozwijania najważniejszych umiejętności w erze sztucznej inteligencji. Trzecia odnosi się do rodzajów kierunków polityki potrzebnych na szczeblu krajowym i unijnym do wsparcia postępów. Zastanawiając się nad pytaniem, jaka wiedza i umiejętności są najbardziej istotne w erze sztucznej inteligencji, Europejski Komitet podkreślił, że cyfryzacja, a zwłaszcza sztuczna inteligencja mają znaczące konsekwencje dla życia codziennego, rozwoju przedsiębiorstw, zatrudnienia i pracy. Chodzi przy tym o wiedzę, zrozumienie i umiejętności. Do odniesienia sukcesu konieczne są wysokiej jakości wiedza, umiejętności i talenty, a także wszechstronna baza wykształconych i wykwalifikowanych osób.

Przedstawione wyżej inicjatywy stały się podstawą dla opracowania „Białej księgi w sprawie sztucznej inteligencji – europejskie podejście do doskonałości i zaufania”[64], którą Komisja Europejska przedstawiła 19 lutego 2020 roku. We wstępie wskazała, że punktem wyjścia do jej opracowania był komunikat

64 COM (2020) 65 final.

Komisji „Sztuczna inteligencja dla Europy", który w „Białej księdze..." został nazwany, z przesadą, „Europejską strategią na rzecz sztucznej inteligencji". Omówienie rozwiązań przyjętych w „Białej księdze..." wykracza poza tematykę niniejszego opracowania, zasługuje jednak na odrębną analizę.

In search of EU artificial intelligence standards

Abstract

Cybersecurity is closely related to the issue of artificial intelligence. The starting point for its presentation in the EU perspective seems to be the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled „Artificial Intelligence for Europe". This communication was preceded by the European Economic and Social Committee's own-initiative opinion „Artificial intelligence: the impact of artificial intelligence on the (digital) single market, production, consumption, employment and society". In the body of this opinion, the European Economic and Social Committee concluded that there is no single accepted and rigid definition of artificial intelligence.

Key words: artificial intelligence, digital market, new technologies

Małgorzata Czuryk*

Employers' provision of access to information necessary to conduct trade union activities

Abstract

Pursuant to Art. 28 of the Trade Union Act of 23 May 1991 (TUA), employers are obliged to provide information necessary to conduct trade union activities at the request of work establishment trade union organisations. The paper defines what information can be requested by a trade union from employers. The author specifies the scope in which the employer examines the request, in what circumstances it may refuse the preparation and transfer of requested information, and what risk it involves.

Key words: work establishment trade union organisation, information, trade union activities, employer, employer's obligations

* Assoc. Prof. Małgorzata Czuryk, PhD, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

Introduction

The legislator defines a trade union as an organisation bringing together employees, established with a view to representing and defending their rights and professional and welfare interests. The subjective dimension of the freedom of association is laid down in Art. 2 of the TUA. The right to establish trade unions is vested in all persons engaged in gainful employment[1]. This includes not only employees but also persons hired on a different basis than an employment relationship, provided that they are paid for their work, do not hire other individuals to perform their tasks, and have employment-related rights and interests which a trade union can deal with. The legislator provides a wide range of individuals and entities that may join trade unions[2]. The legislator's extension of the group of eligible individuals and entities that may form trade unions, or join them, has provided greater opportunities for employed persons to exert pressure on employers to improve their working conditions[3]. The legislator has decided not to regulate the scope of activities performed by work establishment trade union organisations. The lawmakers only indicated that they include, in particular, voicing a trade union's position in individual employee matters insofar as labour law provisions apply and in individual matters of persons engaged in gainful employment in the scope related to the performance of such work; voicing its positions towards the employer or the staff of a self-governing body in matters related to collective interests and the rights of persons engaged in gainful employment; controlling compliance with labour law regulations at the employing establishment, in particular laws and rules governing occupational health and safety; managing the activities of work establishment social labour inspectorates and cooperation with the state labour inspectorate, and dealing with the living conditions of retired employees and disability pensioners[4]. To perform their tasks, trade union organisations have the right to obtain information under

1 Art. 1 of the Trade Union Act of 23 May 1991 (Journal of Laws 2022, item 854), further referred to as the TUA. Cf. K.W. Baran, *Podstawowe zasady zbiorowego prawa pracy* [in:] *System prawa pracy. Część ogólna*, t. 1, ed. idem, Warszawa 2017, p. 1152.

2 Volunteers, trainees and other persons who personally perform work without remuneration may join trade unions in circumstances and under conditions set out in trade union charters, as laid down in Art. 2(4^1) of the TUA.

3 M. Wujczyk, *Nowe regulacje funkcjonowania związków zawodowych – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, vol. 26, no. 3, p. 199.

4 Art. 26 of the TUA.

Art. 28 of the TUA. This means that the bodies of work establishment trade union organisations may unilaterally impose an obligation on the employer's governing bodies and employ the establishment's management bodies to prepare and transfer information[5]. As part of this procedure, information may be requested by a work establishment trade union organisation (which means that a trade union which does not have the status of a work establishment trade union organisation cannot submit such a request). The entitlements in this respect were also granted to inter-enterprise trade union organisations under Art. 34(1) of the TUA[6]. The next section of the paper includes a summary of information which a trade union may request from employers and issues related to an employer's obligation to provide such information.

Information necessary to conduct trade union activities

A trade union organisation may demand from the employer, under Art. 28 of the TUA information required to conduct trade union activities. The provision outlines the example range of information a trade union may request and includes details of working conditions and remuneration rules, the employer's operations and its economic status concerning employment and expected changes in this respect, the status and structure of expected employment changes and measures being undertaken to maintain a given level of employment, and actions which may result in significant changes in work arrangements or the legal basis of employment.

Information about employment conditions should be understood comprehensively. It comprises working arrangements, the work environment, equipment at the employing establishment, access to healthcare services guaranteed by the employer, the provision of commuting possibilities and the possibility to raise one's professional qualifications, working time arrangements, holiday leave, or safe and hygienic working conditions[7]. As regards information about remuneration rules, the right to control compliance with labour laws

5 A. Sobczyk, *Zarys systemu prawa pracy. Ustrój społeczno-gospodarczy III RP i ustrojowe prawo pracy*, t. 2, Kraków 2022, p. 370.

6 B. Surdykowska [in:] P. Czarnecki, P. Grzebyk, A. Reda-Ciszewska, B. Surdykowska, *Ustawa o związkach zawodowych. Komentarz praktyczny z orzecznictwem*, Warszawa 2022, art. 28, Legalis/el.

7 M. Wujczyk, op. cit., p. 206–207.

vested in work establishment trade union organisations also means that they are entitled to control the amounts of employee remunerations. However, it does not entitle them to demand from the employer details of specific employee's remuneration without their consent, as such actions might result in the infringement of an employee's personal interests. According to the Supreme Court, the notion of „information about remuneration rules" should not be applied only to information about laws governing remuneration-setting processes, as these are available to the public. It includes details of specific economic phenomena occurring at an employing establishment, its financial standing and wage bill. Such information may also pertain to the remuneration levels of a specific professional group or remuneration setting rules applicable to specific types of positions[8]. Such information may have varying ranges due to the differing remuneration methods and mechanisms which comprise remuneration systems. For some employers, it may be limited to references to remuneration setting models included in open-access documents, and where there are no internal regulations specifying such rules, it would be necessary to obtain more comprehensive data which could facilitate the understanding of the ways remunerations of specific employee groups are set at the employing establishment. As stated above, it is possible to speak about „information about remuneration rules" insofar as it does not allow the identification of the amount of a salary paid to specific individual employees[9]. The disclosure of individualised information about employees' salaries without their consent might not only result in the infringement of their personal interests. It should be noted that such information is not necessary to conduct trade union activities, neither in respect of group nor individual interests, except where the interests of a specific employee are threatened in relation to the setting of their remuneration for work, and they turn to a trade union to investigate the matter and for the consent for such data to be disclosed. In such an event, the information about the amount of an employee's remuneration is necessary to conduct trade union activities, and the employer is obliged to provide the information to the trade union under Art. 28 of the TUA[10].

8 Resolution of the Supreme Court of 16 July 1993, I PZP 28/93, Legalis no. 28174; Judgement of the Provincial Administrative Court in Poznań of 14 September 2022, IV SA/Po 267/22, Legalis no. 2753825.
9 Ibidem.
10 Ibidem.

Information concerning the operations and economic status of the employer regarding employment and expected changes in this respect refer to the employer's operations, which are related to the management of the employing establishment, its position on the market, its financial standing, and potential changes to the existing operations and economic status which affect its employees' situation[11].

Employment situation should be understood as the number of persons employed under employment relationships and civil-law agreements. Such a listing allows trade unions to identify the actual needs of the employer in respect of the workforce. In addition, the employment structure usually refers to professional groups in service at the employing establishment and the division of employees into specific grades. The information may also refer to employment structure in terms of specified criteria, for instance, age, qualifications or gender[12].

The expected changes to employment refer to the planned, significant increases in the number of employees and the activities which are bound or are likely to result in the reduction of staff[13].

Work establishment trade union organisations may ask the employer to provide information about personnel turnover in relation to their entire staff and individual professional groups[14]. They may also request details of activities aimed at maintaining the current level of employment[15].

Given the above, it is legitimate for a trade union to demand information concerning the total number of employees, the structure of employment basis (employee and non-employee basis); the professional employment structure, personnel turnover ratios, remuneration systems, the principles of setting wage bills, remuneration calculation methods, the methods of dividing a wage bill into payroll and non-payroll funds, wages for individual job positions, the subjective structure of remunerations (e.g. the amount of remuneration for a specific professional group), and the objective structure of remunerations (e.g. the amount of allowances, bonuses, rewards)[16]. It should be stressed here that the criteria the employer has applied to award a pay rise may be necessary

11 M. Wujczyk, op. cit., p. 206–207.
12 Ibidem, p. 207.
13 Ibidem.
14 Ibidem, p. 208.
15 Ibidem.
16 K.W. Baran, *Prawo związków zawodowych do informacji po nowelizacji ustawy związkowej*, „Monitor Prawa Pracy" 2019, no. 1.

for a trade union to fulfil the goal of its activities related to representing and defending employees' rights and their professional and welfare interests. This knowledge might allow the trade union to analyse the compliance of an employer's activities and the situation related to remunerations at the employing establishment with internal and statutory regulations referring to, e.g., equal treatment. It is also assumed that demanding information about the number of persons who received a pay rise within a given group of staff with similar years of service does not constitute reasonable grounds for claiming that they are pieces of information whose provision would be an excessive burden placed on the employer[17]. A trade union may demand „raw" numerical data with a degree of generality that will not result in the disclosure of data of specific employees and which are necessary to conduct trade union activities. According to the case law, for a trade union to perform its statutory tasks and the obligations set out in its charter, it is enough to obtain processed information in the form of statistical data concerning the rules for remunerating individual employee groups[18]. It should also be noted that, in the event a given organisational unit employs a small number of staff members, there is the possibility that the remuneration levels of specific employees might be identified on the basis of data on the remuneration amounts divided by individual units. The literature on the subject includes a position that an employer's provision of such indirect information is not forbidden by law because, in such an event, an employee's right to privacy is not directly infringed by the employer's behaviour[19].

17 M. Rotkiewicz, *Informacje o wynagrodzeniach dla związków zawodowych*, Legalis/el., https://sip-1legalis-1pl-100008dea0b8d.han.uwm.edu.pl/document-full.seam?documentId=mjuwelrsgqydcmzugu4tc&refSource=guide [access: 18.01.2023].

18 Judgement of the Appeals Court in Białystok of 25 June 2014, III AUa 2078/13, Lex no. 1493722.

19 D. Wajda, *Pośrednie wskazanie związkom zawodowym wysokości pensji poszczególnych pracowników*, Legalis/el., https://sip-1legalis-1pl-100008dea0b8d.han.uwm.edu.pl/document-full.seam?documentId=mjuwelrsga2tcmbvge3do&refSource=guide [access: 18.01.2023]. Also, it is worth stressing that measures aimed at counteracting wage discrimination occasionally require an employee to reveal their salary details, even if they are bound by the obligation towards the employer to keep them confidential – H. Szewczyk, *Jawność wynagrodzeń za pracę a unijna zasada „przejrzystości wynagrodzeń" (uwagi de lege lata i de lege ferenda)*, „Praca i Zabezpieczenie Społeczne" 2021, no. 11, p. 5.

The limitations of a trade union organisation's right to demand information

As shown above, the list of information a work establishment trade union organisation may request from an employer is not exhaustive. This means that trade union organisations may request the provision of various pieces of information other than the ones set out in Art. 28 of the TUA, insofar as they are necessary to conduct trade union activities. Therefore, as the legislator has specified that these details should be „information necessary to conduct trade union activities", there is a limitation as to the range of information which a trade union may demand from employers. The fact that the notion used by the legislator is vague poses certain difficulties. Trade unions may demand pieces of information which are objectively related to their activities and are necessary to conduct them[20]. A trade union's right to obtain information necessary to conduct trade union activities comprises all aspects of such operations. A trade union is not entitled to any information which does not serve this purpose, i.e., it is not necessary to conduct trade union activities[21]. However, it may be challenging to identify such purpose in a specific matter, because in practice only trade unions can indicate which information is indispensable in a given situational context. Trade unions are not obliged to substantiate their requests. For that reason, if a given employer has any doubts as to the objectives and, consequently, the legitimacy of providing the requested information, the trade union may be asked to specify in detail the purpose for which such information is necessary. It would facilitate the alignment of the range of data provided for trade union activities[22]. This would need to be carried out before the expiration of the thirty-day time limit for a reply to the request.

The fundamental limit to a trade union's right to demand information from employers under Article 28 of the TAU (as already mentioned) is to specify that it is about information „necessary to conduct trade union activities". Moreover, it is assumed that the right to demand from the employer information necessary to conduct trade union activities is subject to certain

20 Judgement of the Provincial Administrative Court in Gliwice of 9 January 2020, III SAB/Gl 292/19, Lex no. 2777621.

21 L. Florek, *Prawo związku zawodowego do informacji*, „Praca i Zabezpieczenie Społeczne" 2010, no. 5, p. 2–7.

22 K.W. Baran, *Prawo związków zawodowych*...

formal limitations which arise from generally applicable legal regulations[23]. The limits are set out in, i.a., the Act on the Protection of Classified Information[24], the Act on Combating Unfair Competition[25], legal regulations in the sphere of personal data protection[26], the GDPR, and the protection of personal interests or professional secrecy. Before providing requested information, employers should thoroughly analyse the scope of the request and the information to be provided, also in the context of the aforementioned legal acts. They should also consult the issues with their Data Protection Officers because the employer, as the controller of the personal data of its employees, is obliged to take responsibility for the security of the data it processes in relation to employment[27].

According to legal commentators, the Act on the Protection of Classified Information is said to limit trade unions' access to information. It is also noted that in practice, employers seldom inform employee representatives that any given information is treated as classified information within the meaning of the Act on the Protection of Classified Information, with all the implications of the fact[28].

As regards the limits of a request to an employer for information necessary to conduct trade union activities, it should be pointed out that a distinction should be made as to the premises related to the subjective and objective scope of providing information under Art. 28 of the TUA and the Act on the Access to Public Information[29]. The procedures set out in the AAPI and the resulting entitlements are separate and independent of the rights vested in trade unions

23 M. Włodarczyk, *Prawo do informacji* [in:] *System prawa pracy. Zbiorowe prawo pracy*, ed. K.W. Baran, vol. 5, Warszawa 2014, Lex/el.

24 Act of 5 August 2010 on the Protection of Classified Information (consolidated text, Journal of Laws 2019, item 742).

25 Act of 16 April 1993 on Combating Unfair Competition (consolidated text, Journal of Laws 2020, item 1913, as amended).

26 Act of 10 May 2018 on Personal Data Protection (consolidated text, Journal of Laws 2019, item 1781).

27 While providing data, consideration should be given to the fact that the disclosure of an employee's remuneration details without their consent may be treated as infringement of personal interests under Art. 23 and 24 of the Civil Code – Resolution of the Supreme Court of 16 July 1993, I PZP 28/93, Legalis no. 28174.

28 B. Surdykowska, op. cit.

29 The Act of 6 September 2001 on the Access to Public Information (consolidated text, Journal of Laws 2022, item 902), further referred to as the AAPI.

pursuant to the TUA[30]. Under the TUA, only the employer is an entity obliged to provide information under the TUA, and the information such an employer discloses is not categorised as public information and does not need to concern public matters. At the same time, the indispensability of such information to conduct trade union activities is a prerequisite for its disclosure. Trade union organisations are entitled to demand from the entity information which has the properties of public information according to the AAPI[31]. A trade union organisation can choose the procedure for requesting information. The status of a trade union does not mean that the application of the AAPI is excluded[32]. The case law also demonstrates a more restrictive view, stating that if public information is the object of the request, Art. 28 of the TUA is not applicable in such a matter, and the entity concerned has no grounds to invoke limitations arising from the said legal provision[33]. The procedure provided for in this legal regulation is independent of the one guaranteed in the Act on the Access to Public Information. It constitutes *lex specialis* concerning the latter Act and is not subject to assessment as part of access to public information[34].

Employer's obligation to provide information

If under Art. 28 of the TUA, the data a trade union requests is related to the objectives of trade union activities pursued by such an organisation, the employer concerned is obliged to provide access to it. The verification of the objectives of trade union activities may be problematic at times, as only the trade union can identify the data which are necessary for a specific situation. As indicated above, if the employer has any doubts, it may consider submitting a request to provide additional details of the purpose for which the given information is requested within 30 days of the trade union's request.

30 Judgement of the Provincial Administrative Court in Poznań of 3 December 2021, IVSA/PO 817/21, Lex no. 2650485.

31 Ibidem.

32 Judgement of the Provincial Administrative Court in Warsaw of 16 April 2020, VIII SAB/Wa 7/20, Legalis no. 2419956.

33 Judgement of the Provincial Administrative Court in Łódź of 18 July 2019, II SA/Łd 310/19, Legalis no. 2195477.

34 Judgement of the Provincial Administrative Court in Opole of 21 December 2018, II SAB/Op 111/18, Legalis No. 1867088.

Furthermore, the employer may refuse to provide information if, for example, it has reasons to suspect that the information which the trade union requests is not directly related to the activities of the trade union and will be used for political, publicity or particularistic purposes, or that its range clearly goes beyond the statutory obligation to keep trade unions informed[35]. It should be clarified that it is the employer who bears the risk of the wrong assessment of the request. Thus, the failure to provide information (or disclosing incomplete or inaccurate information) or the failure to provide it on time (within 30 days of the receipt of the request), although not penalised directly, may be classified as hindering trade union activities conducted in line with the provisions of the Act and result in liability under Article 35(1)(2) of the TUA. Such conduct may be punishable by a fine or the restriction of liberty.

Bibliography

Baran K.W., *Podstawowe zasady zbiorowego prawa pracy* [in:] *System prawa pracy. Część ogólna*, t. 1, ed. K.W. Baran, Warszawa 2017.

Baran K.W., *Prawo związków zawodowych do informacji po nowelizacji ustawy związkowej*, „Monitor Prawa Pracy" 2019, no. 1.

Czarnecki P., Grzebyk P., Reda-Ciszewska A., Surdykowska B., *Ustawa o związkach zawodowych. Komentarz praktyczny z orzecznictwem*, Warszawa 2022.

Florek L., *Prawo związku zawodowego do informacji*, „Praca i Zabezpieczenie Społeczne" 2010, no. 5.

Rotkiewicz M., *Informacje o wynagrodzeniach dla związków zawodowych*, Legalis/el., https://sip-1legalis-1pl-100008dea0b8d.han.uwm.edu.pl/document-full.seam?documentId=mjuwelrsgqydcmzugu4tc&refSource=guide [access: 18.01.2023].

Sobczyk A., *Zarys systemu prawa pracy. Ustrój społeczno-gospodarczy III RP i ustrojowe prawo pracy*, t. 2, Kraków 2022.

Szewczyk H., *Jawność wynagrodzeń za pracę a unijna zasada „przejrzystości wynagrodzeń" (uwagi de lege lata i de lege ferenda)*, „Praca i Zabezpieczenie Społeczne" 2021, no. 11.

Wajda D., *Pośrednie wskazanie związkom zawodowym wysokości pensji poszczególnych pracowników*, Legalis/el., https://sip-1legalis-1pl-100008dea0b8d.han.uwm.edu.pl/document-full.seam?documentId=mjuwelrsga2tcmbvge3do&refSource=guide [access: 18.01.2023].

Włodarczyk M., *Prawo do informacji* [in:] *System prawa pracy. Zbiorowe prawo pracy*, ed. K.W. Baran, vol. 5, Warszawa 2014.

Wujczyk M., *Nowe regulacje funkcjonowania związków zawodowych – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019, vol. 26, no. 3.

35 K.W. Baran, *Prawo związków zawodowych*…

Udostępnienie przez pracodawcę informacji niezbędnych do prowadzenia działalności związkowej

Streszczenie

Zgodnie z treścią art. 28 ustawy z 23 maja 1991 roku o związkach zawodowych, pracodawca ma obowiązek udzielić na wniosek zakładowej organizacji związkowej informacji niezbędnych do prowadzenia działalności związkowej. W artykule wskazano, o jakie informacje związek zawodowy może zwracać się do pracodawcy. Określono, w jakim zakresie pracodawca bada wniosek i w jakich sytuacjach oraz z jakim ryzykiem może odmówić przygotowania i przekazania zawnioskowanych informacji.

Słowa kluczowe: zakładowa organizacja związkowa, informacje, działalność związkowa, pracodawca, obowiązki pracodawcy

Kazimierz J. Pawelec*

Zmiana polityki karania w nowelizacji kodeksu karnego z 7 lipca 2022 roku. Uwagi krytyczne

Streszczenie

Tworzenie prawa to jak rozwiązywanie zagadek kryminalnych. Parafrazując Avi Loeba, ustawodawca musi podążać tam, dokąd prowadzą go dowody. Tymi dowodami są dane empiryczne, badania naukowe, a zwłaszcza ich osiągnięcia. Podążanie za powyższymi wymaga pokory, która wyzwala z uprzedzeń mogących wpływać na obserwacje i wnioski. Tworzenie norm karnych to przede wszystkim próba systemowego podejścia, żeby ów system był spójny, przede wszystkim zapobiegał, a dopiero na końcu karał przy indywidualnym podejściu do sprawcy, któremu udowodniono winę z zachowaniem wszystkich gwarancji przysługujących stronom postępowania w uczciwym procesie. Analizując zmiany w uchwalonej nowelizacji, autor skupił się na sprawcach nieletnich i młodocianych popełniających również przestępstwa, tj. wypadki drogowe, rzadziej katastrofy bądź sprowadzenia ich bezpośredniego niebezpieczeństwa. Ich przyczynami częstokroć były niezwykle ryzykanckie zachowania, agresja, a nawet furia drogowa. Czy za skutki tych czynów sprawcy powinni być karani z całą surowością, jak to uchwalił parlament? Krytyczna ocena zmiany filozofii karania jest przedmiotem rozważań autora niniejszego artykułu.

Słowa kluczowe: zasady karania, prewencja szczególna i ogólna, nieletni i młodociani sprawcy

* Dr Kazimierz J. Pawelec, adwokat, Okręgowa Rada Adwokacka w Warszawie, adiunkt, Instytut Nauk o Bezpieczeństwie, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, ORCID: 0000-0001-8669-0249.

Wstęp

Uchwalona 7 lipca 2022 roku nowelizacja przepisów kodeksu karnego (k.k.) znacznie podwyższyła kary za groźne – zdaniem ustawodawcy – przestępstwa. Chodziło o: nieumyślne spowodowanie śmierci (art. 155), zarażenie wirusem HIV, chorobą weneryczną lub zakaźną bądź nieuleczalną, w tym także zagrażającą życiu (art. 161), piractwo (art. 166 § 1), handel ludźmi (art. 189a), tzw. twardą pornografią (art. 202) i zmuszaniem do prostytucji w typie kwalifikowanym (art. 203 § 2) i inne.

Parlamentarzyści, mimo negatywnych opinii specjalistów, założyli, że wyłącznie surowe kary pozbawienia wolności spowodują spadek przestępczości. To pogląd zgoła ze średniowiecza, kiedy to surowe karanie, w tym kwalifikowanymi, publicznie wykonywanymi m.in. karami śmierci, było powszechne. Czy to odstraszało mimo dużej pomysłowości podczas wykonywanych egzekucji? Absolutnie nie. Podobnie jest z karą dożywotniego pozbawienia wolności przy ograniczeniu warunkowego przedterminowego zwolnienia dopiero po upływie 30 lat z zastrzeżeniem, że okres próby będzie trwał dożywotnio. Podobnie jest, chociaż jest to problem bardziej złożony, o czym będzie mowa dalej, w przypadku pociągania do odpowiedzialności karnej 14-latków za niektóre rodzaje zabójstw czy też kar dotyczących pijanych lub odurzonych kierowców. Tak samo będą traktowani gwałciciele, którzy nagrywali popełnione przez siebie przestępstwa. Zdaniem 229 parlamentarzystów głosujących za uchwaleniem tego rodzaju rozwiązań wyłącznie surowa kara będzie remedium na potencjalnych sprawców. Nic bardziej błędnego. Pomijając już ogląd statystyki przestępczości, która co roku maleje. Parlament, w ślad za projektem Ministerstwa Sprawiedliwości, pozostał głuchy na wyniki badań naukowych czy też doświadczenia judykatury. Przyjął, chociaż tego wprost nie wyartykułował, że odosobnione, rażące przypadki zbrodni czy innych przestępstw stanowią podstawę do naruszenia i tak mało stabilnego porządku prawnego, a także wywrócenia filozofii karania do góry nogami. Owe anomalie zostały przyjęte jako reguła, mimo że świat nauki anomalie z reguły traktował jako ekscesy, które w skali społecznej nie były brane pod uwagę lub tylko sygnalizowane. Tymczasem nowelizacja z 7 lipca 2022 roku potraktowała je jako regułę, co z punktu widzenia kryminologii, a także innych dyscyplin naukowych może przyprawić o zawrót głowy.

Autor niniejszej publikacji pragnie skupić się na kwestiach związanych z zaostrzeniem odpowiedzialności karnej kierujących pojazdami mechanicznymi za wypadki bądź inne zdarzenia drogowe, nie zapomina jednak o innych,

w stosunku do których nowela zaostrzyła powszechnie rozumianą odpowiedzialność wręcz do rozmiarów drakońskich. Zasadniczo zwrócił uwagę na grupę, można rzec, przypadkowych sprawców przestępstw nieumyślnych, najbardziej demokratycznych we współczesnym świecie, ponieważ mogą one dotknąć każdego, a zagrożenie i ryzyko wzrasta wprost proporcjonalnie do liczby przejeżdżanych kilometrów.

Bat na kierowców

Uchwalona nowelizacja kodeksu karnego przewiduje także nadzwyczajne obostrzenie kar w stosunku do sprawców przestępstw przeciwko bezpieczeństwu w komunikacji określonych w art. 178 k.k. Ma ona dotyczyć również sprawców, którzy bezpośrednio po popełnieniu w stanie nietrzeźwości wypadku drogowego, katastrofy czy sprowadzenia jej bezpośredniego niebezpieczeństwa spożyli alkohol lub zażyli środki odurzające w celu uniknięcia bardziej surowej odpowiedzialności karnej. Ciekawe jak tego rodzaju regulacja ma się do zasady *nemo se ipsum accusare tenetur* (nikt nie ma obowiązku dostarczania dowodów przeciwko sobie), prawa do obrony, uprawnień procesowych oskarżonych, które wyraźnie zostały określone w Konstytucji RP, ratyfikowanych umowach międzynarodowych czy też procedurze karnej (art. 71 § 1 k.p.k.)?

Ustawodawca przewidział również podwyższenie zagrożenia karnego za prowadzenie pojazdu mechanicznego w stanie nietrzeźwości lub pod wpływem środków odurzających (art. 178a § 1 k.k.). I dalej, w razie popełnienia występku z art. 178a § 1 k.k., jeżeli w organizmie sprawcy zawartość alkoholu była nie mniejsza niż 1,5 promila we krwi lub 0,75 mg/dec^3 w wydychanym powietrzu, sąd orzeka przepadek prowadzonego przez niego pojazdu mechanicznego bądź przepadek jego równowartości. Wydawać się może, że to czyste kuriozum. Co ma wspólnego z przestępstwem współwłaściciel, np. współmałżonek, czy inna Bogu ducha winna osoba? Czy też jak praktyka potraktuje amerykańskiego żołnierza, który w stanie nietrzeźwości wyjechał czołgiem i został schwytany? Czy zabierzemy czołg jednostce, a żołnierz niech płaci? Ten nieprawdopodobny pomysł, który był zgłaszany przed laty, został w końcu zrealizowany w sposób absolutnie bezkrytyczny.

Przytoczone nowe regulacje karne mogą i powinny budzić poważne wątpliwości. Godzi się podkreślić, że skutek wypadku drogowego czy innego przestępstwa skierowanego przeciwko bezpieczeństwu w komunikacji to czysty przypadek. Sprawcy oraz ofiary nie łączy (oprócz nielicznych wyjątków) żadna

relacja psychiczna. Co więcej, gros wypadków drogowych o bardzo spektakularnym charakterze, połączonych z umyślnym naruszeniem zasad bezpieczeństwa, popełniają młodzi, niedoświadczeni kierowcy. Czy oni, niejako z automatu, powinni być traktowani z pełną surowością niczym zabójcy? Problem ten ustawodawca pominął milczeniem, chociaż jest on niezwykle istotny z punktu widzenia polityki karania.

Rzecz o młodocianych sprawcach

Według statystyk policyjnych w 2021 roku na polskich drogach doszło do 32 760 wypadków. Najliczniejszą grupę sprawców stanowili kierowcy w wieku od 18 do 24 roku życia. Zarzucono im popełnienie 5500 wypadków drogowych, w których zginęło 468 osób, a 7272 zostało rannych[1].

Mniejsza o podanie określonych przez Policję przyczyn w sposób niezwykle rygorystyczny i formalny właściwy dla prawa administracyjnego. Istota problemu sprowadzała się do ustalenia przyczyn spowodowania przez wymienionych, młodych kierowców, stanów zagrożenia, a także, w razie przypisania im winy, dobrania odpowiedniej „terapii" karnej. Nie sposób przy tym pominąć, że doświadczenie oraz dojrzałość tych młodych kierujących należała do mniej niż skromnych. Powyższe należało również połączyć z brakiem kwalifikacji, której jeszcze nie posiedli mimo odbycia szkolenia, zdania egzaminu państwowego oraz uzyskania prawa jazdy. Dotychczasowa praktyka brak doświadczenia traktowała wyłącznie jako względną okoliczność łagodzącą. Sąd Najwyższy w wyroku z 12 lipca 1975 roku (V KRN 65/75, OSNKW 1975, nr 12, poz. 160) przyjął, że brak doświadczenia może być uwzględniony na korzyść kierowcy wówczas, gdy stanął on w obliczu zaskakującej sytuacji drogowej, której nie mógł sprostać. Z kolei w wyroku Sądu Najwyższego z 16 marca 1979 roku (V KRN 93/79, OSNPG 1979, nr 11, poz. 148) czytamy: „[…] skoro spowodowany przez oskarżonego wypadek był wynikiem świadomego przewożenia na motocyklu zamroczonego alkoholem pasażera i umyślnego naruszenia zasad ruchu drogowego, toteż brak doświadczenia oskarżonego, który niedawno

1 https://szukaj.onet.pl/wyniki/?qt=statystyki%20policyjne%20wypadk%C3%B3w%20drogowych#gsc.tab=1&gsc.q=statystyki%20policyjne%20wypadk%C3%B3w%20drogowych&gsc.page=1 [dostęp: 15.07.2022].

nabył uprawnienia do kierowania pojazdami mechanicznymi, zobowiązywał go do ostrożnej jazdy i przestrzegania przepisów ruchu drogowego”[2].

W tym miejscu nie możemy pominąć, że młodych kierowców cechuje, a wskazuje na to praktyka, częstokroć podejmowanie ryzykownych decyzji powodujących bezpośrednie niebezpieczeństwo spowodowania wypadku, katastrofy czy sprowadzenia realnego niebezpieczeństwa jej nastąpienia. Łączą się z tym wielokrotnie nieprzestrzeganie ograniczeń prędkości czy wręcz agresja w ruchu drogowym. Ową agresję, a czasami furię drogową możemy łączyć m.in. z właściwościami psychofizycznymi i psychologicznymi[3]. Nie sposób w tym miejscu pominąć wyników badań Russella A. Poldracka, który pisał: „[…] z badań psychologicznych wynika, że do ustalenia, że możliwość kontrolowania własnych umysłów jest u nastolatków (przeciętnie) osłabiona, a co za tym idzie nie można pociągać ich do odpowiedzialności za popełnione czyny”[4]. Dalej autor przytaczał sprawy, w których sądy Stanów Zjednoczonych Ameryki zauważyły, że „[...] rozwój psychologii i nauki o mózgu ciągle pokazuje fundamentalne różnice między umysłami młodocianych i dorosłych. Na przykład, części mózgu zaangażowane w kontrolę zachowania wciąż rozwijają się w końcowym okresie dojrzewania”[5]. Autor przytoczył przykłady wielu rozstrzygnięć sądowych, które zaufały badaniom neuroobrazowym wystarczającym do tego, żeby na ich podstawie podjąć decyzje dotyczące życia lub śmierci podsądnych.

Obserwując praktykę, warto zwrócić uwagę, że neuronauka dostarczała wiedzy, że mózg nastolatka (18 lat–24 lata) nie jest jeszcze dobrze rozwinięty i, jak zauważył William Shakespeare, „[...] żeby tak między dziesiątym rokiem a dwudziestym trzecim w ogóle nie było albo żeby młodzież cały ten czas przesypiała; bo nic się w nim nie dzieje, tylko robieniem dziewuchom dzieciaków, brak uważania dla starszych, złodziejstwo i bijatyki”[6].

Badania neuroobrazowe dostarczają coraz wyraźniejszego obrazu, dlaczego nastolatki zachowują się tak, jak się zachowują.

2 Więcej na ten temat zob.: K.J. Pawelec, *Bezpieczeństwo i ryzyko w ruchu drogowym*, Warszawa 2020, s. 150–151 oraz podana literatura i orzecznictwo; idem, *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2021, s. 517–545 wraz z podanym orzecznictwem i literaturą.

3 Więcej na ten temat zob. K.J. Pawelec [w:] *Wypadki i inne zdarzenia drogowe. Opiniowanie w sprawach rekonstrukcji*, red. idem, P. Krzemień, Warszawa 2020, s. 130–141 oraz podana literatura.

4 R.A. Poldrack, *The new mind readers. What neuroimoging can and canonot reveal abouth our thoughts*, Standford 2018, s. 144.

5 Ibidem.

6 W. Shakespeare, *Burza. Zimowa opowieść*, tł. S. Barańczak, Kraków 1991, s. 203

W swojej praktyce, niestety, jeszcze nie spotkałem się z opinią biegłego psychologa, który na podstawie neuroobrazowania mózgu, co także nigdy nie było wnioskowane przez biegłych psychiatrów, wydał opinię związaną ze stanem poczytalności sprawcy. Myślę, że warto sięgać po tego rodzaju dowód, zwłaszcza w odniesieniu do nastolatków, którym zarzucono popełnienie czynów przestępczych, według wszystkich rozsądnych ludzi, zupełnie w sposób irracjonalny i kompletnie niezrozumiały.

Garść refleksji

Ponownie należy przytoczyć pogląd Poldracka, który pisał: „Jedno z podstawowych wyzwań związanych z wykorzystaniem nauki w kwestiach prawnych polega na tym, że nauka i prawo mają pod wieloma względami diametralnie różne cele. Prawo i neuronauka oczywiście dążą do prawdy, ale prawdy różnego rodzaju. Naukowcy zazwyczaj dążą do odkrycia ogólnych prawd, które odnoszą się do całej populacji […]. Z kolei prawo musi podejmować ostateczne i definitywne decyzje w indywidualnych przypadkach”[7].

Trudno polemizować z autorem przytoczonego poglądu. Wymaga on jednak modyfikacji. Prawo nie może być głuche na zdobycze wiedzy, osiągnięcia nauki, doświadczenia praktyki, nowe metody badawcze itd. Musi po nie sięgać, i to pełnymi garściami, i wykorzystywać podczas procesu legislacyjnego przez władze ustawodawcze. Prawo musi być akceptowane przez ogół społeczności, traktowane jako uczciwe i sprawiedliwe. Tymczasem ustawodawca w ostatniej nowelizacji kodeksu karnego dążył wyłącznie do wywołania w społeczeństwie paroksyzmu strachu, w tym także w odniesieniu do przypadkowych sprawców przestępstw, zwłaszcza młodocianych. Nie zauważył, że etiologia przestępczości komunikacyjnej dotychczas nie została zbadana, a jest ona nauką wybitnie interdyscyplinarną. Nie dostrzegł podstawowego problemu, że stanowi ona nieodłączną triadę: człowiek–pojazd–droga. Tym samym nawet nie próbował podjąć jakichkolwiek działań eliminujących niebezpieczeństwo, potraktował wyłącznie człowieka jako najsłabsze ogniowo systemu[8].

Niebezpieczeństwo leżące na przedpolu wszelkiej przestępczości komunikacyjnej powinno zostać na podstawie dociekań naukowych dokładnie

7 R.A. Poldrack, op. cit., s. 144.

8 Por. A. Gaberle, *Najsłabsze ogniwo (człowiek jako źródło zagrożeń w ruchu drogowym)*, Warszawa 1986, s. 15.

zbadane oraz precyzyjnie określone. Wzmożona represyjność, podobnie jak przeprowadzane akcje propagandowe, trafiają w próżnię. To nie są skuteczne metody. Działalność prawotwórcza powinna zmierzać do wyeliminowania wskazanego niebezpieczeństwa. Tworzenie prawa to coś, jakby rozwiązywanie zagadek kryminalnych. Parafrazując Loeba, ustawodawca musi podążać tam, dokąd prowadzą go dowody. Podążanie za danymi empirycznymi wymaga pokory, która wyzwala z uprzedzeń mogących wpływać na obserwacje i wnioski. Podobnie jest, i było, z korzystaniem z osiągnięć nauki, i to z bardzo różnych dziedzin. Tworzenie norm karnych to przede wszystkim próba systemowego podejścia, żeby zapobiegał, a dopiero na końcu karał z indywidualnym podejściem do sprawcy, któremu udowodniono winę, z zachowaniem wszystkich gwarancji w uczciwym procesie[9].

Jeżeli chodzi o człowieka, sprawcę przestępstwa komunikacyjnego, to warto zaprzestać traktowania go jako najsłabsze ogniwo systemu. Organy władzy publicznej powinny w końcu dostrzec, że one także ponoszą odpowiedzialność za skutki wypadków oraz innych zdarzeń drogowych.

Kilka propozycji, czyli rzecz o postulatach *de lege ferenda*

Działania zapobiegawcze, eliminujące zagrożenia w ruchu drogowym, powinna realizować ustawa z 20 czerwca 1997 roku – Prawo o ruchu drogowym (Dz.U. 1997, nr 98, poz. 602, z późn. zm.). Jest to akt prawny niezwykle obszerny, co wynikało z wielu przyczyn. Na plan pierwszy wysuwała wielość podmiotów oraz zakres regulacji, metodykę legislacyjną, a także rozwlekłość języka. Jest to akt prawny mało czytelny, niewiele ustępujący objętością kodeksowi postępowania karnego, dlatego mało komunikatywny. Przepisy regulujące ruch drogowy znajdują się w dwóch pierwszych działach prawa o ruchu drogowym. Ich kodyfikacja jest wadliwa zarówno pod względem merytorycznym, jak i legislacyjnym. Aktualny pozostaje pogląd Aleksandra Bachracha, który przed laty pisał: „[…] Kazuistyczne przepisy, wyrażone w sposób opisowo-szkoleniowy, nie zaś prawno-dydaktyczny, pozbawione są logicznie uzasadnionej systematyki. Nie wyrażają elementarnych zasad ruchu oraz zasad ostrożności.

9 A. Loeb, *Pozaziemskie. Pierwsze ślady życia rozumnego poza Ziemią*, przekł. M. Krośniak, T. Tesznar, Poznań 2021, s. 29.

Zawierają dyrektywy wewnętrznie sprzeczne i niesprawiedliwe z punktu widzenia zasad dobrej roboty”[10].

Wiele niejasności wywołują przepisy dotyczące tak typowych manewrów jak wyprzedzanie i omijanie. Te opisowo i rozwlekle zredagowane normy starają się wskazywać wszystko to, co może kierowcę spotkać na drodze. Ich normy zmierzają do określonego celu, ale nie dostrzegają skutków ubocznych, które nie były zamierzone. Podobnie jest z przepisami dotyczącymi hamowania, bezpiecznego odstępu od poprzednika czy jazdy możliwie blisko prawej krawędzi, a także relacji pojazd–pieszy na przejściu. Ten ostatni przepis wywołał moc nieporozumień, gdyż nie jest prawdą, że pieszy ma bezwzględne pierwszeństwo na przejściu. Owszem, korzysta ze szczególnej ochrony w razie wkroczenia na nie, ale z zachowaniem szczególnej ostrożności i zakazu wkraczania w bezpośredniej bliskości nadjeżdżającego pojazdu. Z kolei na kierującego został nałożony obowiązek zachowania szczególnej ostrożności i odpowiedniego zmniejszenia prędkości. Ale do jakiej? Powyższe może wprost prowadzić do automatyzacji odpowiedzialności karnej kierującego. I dalej, niewątpliwie zasadny jest obowiązek zachowania określonego odstępu kierującego samochodem od wymijanego czy wyprzedzanego jednośladu, ale dlaczego taki obowiązek nie dotyczy kierujących tych ostatnimi? Odpowiedzi nie znamy.

Z przedstawionego wywodu płynie wniosek o konieczności gruntownej zmiany przepisów prawa o ruchu drogowym, kładącego nacisk na eliminowanie zachowań i sytuacji wywołujących niebezpieczeństwo, zwłaszcza przez kategoryczne określenie powinności poszczególnych uczestników ruchu, przede wszystkim w sytuacjach kolizyjnych, bez posługiwania się asekuracyjnym podejściem do sytuacji wymagających jednoznacznego potraktowania, np. określenia obowiązków wyprzedzającego i wyprzedzanego, manewru omijania, zmiany pasa ruchu, hamowania czy wreszcie relacji pojazd–pieszy na przejściu. W tym ostatnim przypadku nałożenie obowiązku odpowiedniego zmniejszenia prędkości nie może być uznane za uczciwe, gdyż może prowadzić, a niestety tak się dzieje w praktyce, do automatyzacji odpowiedzialności karnej, dlatego że każda prędkość może okazać się nieodpowiednia, ponieważ doszło do potrącenia. Czyż nie lepiej byłoby, gdyby została ona konkretne określona, np. do 30 km/h, co nie wymagałoby jakiejkolwiek interpretacji.

10 A. Bachrach, *Przestępstwa i wykroczenia drogowe w prawie polskim*, Warszawa 1980, s. 218 i nast.

Kolejnym problemem są kwestie związane z koniecznością eliminowania z ruchu niebezpiecznych kierowców. Chodzi o to, żeby byli oni z odpowiednim wyprzedzeniem wyłączani z ruchu. W tej materii, niejako *post factum*, nie trzeba konfiskować im pojazdów, ale zasadne jest znaczne zaostrzenie kryteriów związanych ze stanem zdrowia czy właściwościami psychologicznymi zanim takie osoby uzyskają uprawnienia do kierowania pojazdami mechanicznymi. Można postulować, żeby ubiegający się o uzyskanie prawa jazdy, także kat. A i B, obowiązkowo był poddawany badaniom psychologicznym oraz badano ich krew bądź wydzieliny organizmu na obecności substancji zabronionych, osłabiających zdolności psychomotoryczne, a w szczególnie uzasadnionych przypadkach także badaniom psychiatrycznym.

W obowiązującym stanie prawnym, a dowodzi tego praktyka, nie jest wielkim problemem, żeby prawo jazdy kat. A lub B uzyskała osoba cierpiąca na chorobę alkoholową czy uzależniona od środków odurzających bądź psychotropowych, chora psychicznie lub na inne schorzenia determinujące ordynowanie leków osłabiających sprawności psychomotoryczne. Z kolei badania psychologiczne okazują się niezbędne do określenia poziomu intelektualnego, poznania osobowości, ze szczególnym uwzględnieniem zachowania w sytuacjach trudnych, stresujących, oraz poziomu dojrzałości społecznej[11].

W obowiązującym systemie prawnym jest dostrzegana dysharmonia rozróżniająca cztery pojęcia związane ze spożycie alkoholu bądź zażyciem środka odurzającego. Dwa z nich stanowią znamiona wykroczenia z art. 87 § 2 k.w. (znajdowania się kierującego pojazdem mechanicznym w stanie wskazującym na użycie alkoholu lub podobnie działającego środka), również dwa wyczerpują znamiona przestępstwa z art. 178a § 1 k.k. (stan nietrzeźwości lub pod wpływem środka odurzającego). Tolerowanie wskazanej dysharmonii nie jest niczym uzasadnione. Stąd racjonalny jest postulat *de lege ferenda* wprowadzenia, wzorem innych krajów, zerowej tolerancji na zawartość alkoholu oraz związków z grupy opiatów i innych w organizmie kierującego.

Ważna jest także kwestia dostrzegana w praktyce, a niezauważana przez ustawodawcę, że wiele zachowań w ruchu drogowym stwarzających niebezpieczeństwo nie wyczerpuje dyspozycji art. 174 k.k. (sprowadzenie realnego niebezpieczeństwa nastąpienia katastrofy), ale ładunek społecznego i realnego niebezpieczeństwa absolutnie nie przystaje do wykroczenia z art. 86 k.w.

11 Więcej na ten temat zob. K.J. Pawelec, *Bezpieczeństwo i ryzyko*…, s. 342–345. Por. idem, *Prawo o ruchu drogowym. Zasady bezpieczeństwa. Komentarz*, Warszawa 2005, s. 182.

(spowodowanie zagrożenia bezpieczeństwa w ruchu drogowym). Brakuje w ustawie karnej przepisu wypełniającego tę lukę. Można zaproponować *de lege ferenda* uzupełnienie treści art. 174 § 1 k.k. przez dopisanie wypadku z art. 177 k.k.

Wydaje się, że warto rozważyć możliwość orzekania środka karnego zakazu prowadzenia pojazdów mechanicznych również z warunkowym zawieszeniem jego wykonania. Tak zaproponowana forma wskazanego środka karnego zapewne spotka się ze społeczną aprobatą, zmniejszy automatyzm jego orzekania, a także będzie spełniała ważną funkcję profilaktyczną podnoszącą bezpieczeństwo drogowe.

Na zakończenie warto zwrócić uwagę, że powyższe może stanowić raczej postulaty *de lege lata* adresowane do praktyki, a związane z zupełnym nierozważeniem kwestii dotyczących braków bezpieczeństwa biernego pojazdów oraz ich rozważeniem w kontekście istnienia adekwatnego związku przyczynowego ze skutkami wypadków czy katastrof drogowych. Można wprost postawić pytanie, czy wskazane braki tego bezpieczeństwa, istotnego dla eliminowania skutków, powinny obciążać winnych naruszenia zasad bezpieczeństwa w zakresie możliwości oraz powinności ich przewidzenia? Wydaje się, że obciążanie tymi skutkami z punktu widzenia adekwatnego związku przyczynowego nie znajduje racjonalnego uzasadnienia, a przynajmniej powinno być przedmiotem dowodzenia, co zasadniczo nie jest czynione. Podkreślić przy tym należy, że w ciągu ostatnich 10 lat Polacy sprowadzili z zagranicy ponad 8 mln używanych samochodów, z reguły bardzo leciwych[12].

Ile z tych aut nie odpowiadało wymogom bezpieczeństwa biernego? Niestety, nie wiadomo, dlatego że nikt nie interesował się tym problemem. Nie interesowała się tym ani Policja, ani inne służby organów państwa, w tym służb zajmujących się dopuszczeniem do ruchu sprowadzonych z zagranicy używanych samochodów. Problem ten dostrzegł Damian Klewek w pracy pt. „Dopuszczenie pojazdów mechanicznych do ruchu i jego znaczenie dla bezpieczeństwa komunikacji drogowej", obronionej na Wydziale Nauk Ekonomicznych i Prawnych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach w lipcu 2019 roku. Autor trafnie zauważył (s. 32–33, niepubl.), że stacje diagnostyczne powinny być wyposażone w odpowiedni sprzęt umożliwiający zbadanie sprawności urządzeń zapewniających bezpieczeństwo bierne, co powinno być połączone ze zmianami legislacyjnymi.

12 A. Kubiak, *Polska ściąga auta z całego świata*, „Gazeta Wyborcza" 2019, nr z 15 lipca.

Podobnie należy potraktować problematykę odpowiedniego wyposażenia dróg, ich oznakowania, inżynierii ruchu. Odpowiedzialni funkcjonariusze państwa powinni być otwarci na sygnały służb odpowiedzialnych za bezpieczeństwo ruchu, a w krańcowych przypadkach nie może być wykluczona ich odpowiedzialność karna z art. 231 k.k.

Jednakże kwestie te wkraczają poza zakres niniejszej publikacji, chociaż są godne zainteresowania badaczy, czego dotychczas nie czyniono.

Bibliografia

Bachrach A., *Przestępstwa i wykroczenia drogowe w prawie polskim*, Warszawa 1980.
Gaberle A., *Najsłabsze ogniwo (człowiek jako źródło zagrożeń w ruchu drogowym)*, Warszawa 1986.
Kubiak A., *Polska ściąga auta z całego świata*, „Gazeta Wyborcza" 2019, nr z 15 lipca.
Loeb A., *Pozaziemskie. Pierwsze ślady życia rozumnego poza Ziemią*, przekł. M. Krośniak, T. Tesznar, Poznań 2021.
Pawelec K.J., *Bezpieczeństwo i ryzyko w ruchu drogowym*, Warszawa 2020.
Pawelec K.J., *Prawo o ruchu drogowym. Zasady bezpieczeństwa. Komentarz*, Warszawa 2005.
Pawelec K.J., *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych*, Warszawa 2021.
Poldrack R.A., *The new mind readers. What neuroimoging can and canonot reveal abouth our thoughts*, Standford 2018.
Shakespeare W., *Burza. Zimowa opowieść*, tł. S. Barańczak, Kraków 1991.
Wypadki i inne zdarzenia drogowe. Opiniowanie w sprawach rekonstrukcji, red. K.J. Pawelec, P. Krzemień, Warszawa 2020.

The change in punitive policy in the amendment to the Penal Code of 7 July 2022. Critical comments

Abstract

Law making is akin to solving criminal puzzles. To paraphrase A. Loeb, the legislator must follow the evidence. The evidence includes empirical data, scientific research and especially the achievements of researchers. Following the above requires humility, which frees one from biases that can affect one's observations and conclusions. Creating norms of penal law consists most of all of a systemic approach, so that this system is consistent and, most importantly, only at the end of proceedings punishes with an individual approach the offender whose guilt has been proven with all the guarantees afforded to the parties in the proceedings of a fair trial. Analysing the changes in the enacted amendment, the author focused on minor and juvenile offenders who also committed crimes, i.e. traffic accidents and, less frequently, traffic disasters or causing the immediate danger thereof. They were often an effect of extremely risky behaviour, aggression and even road rage. Should these perpetrators be punished for the consequences of these acts with all the tightened severity, as enacted by Parliament? A critical assessment of the change in punishment philosophy deserves consideration.

Key words: principles of punishment, specific and general prevention, minor and juvenile perpetrators

Jakub Skłodowski*
Piotr Arabas**

Wykorzystanie drzew sufiksowych do efektywnej prezentacji podobieństw sesji z systemu pułapek honeypot

Streszczenie

W artykule przestawiono prototyp systemu do analizy danych z sieci interaktywnych pułapek, tzw. honeypotów. Szczególną uwagę zwrócono na algorytm wyszukiwania podobieństw w zbieranych zapisach sesji ssh. Algorytm ten wyszukuje w sesjach uogólnione wzorce z wykorzystaniem drzew sufiksowych. Wzorce te dzięki zaproponowanej metodzie redukcji mogą być następnie wykorzystane do wygodnej prezentacji zarejestrowanych sesji i efektywnego wyszukiwania. Podsumowanie pracy stanowią przykłady wykorzystania algorytmu.

Słowa kluczowe: honeypoty, malware, analiza sesji, drzewa sufiksowe

* Jakub Skłodowski, inżynier oprogramowania, Dział Systemów Bezpieczeństwa Sieci, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, e-mail: Jakub.Sklodowski@nask.pl.
** Piotr Arabas, adiunkt, Dział Systemów Bezpieczeństwa Sieci, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, e-mail: Piotr.Arabas@nask.pl.

Wstęp

W ostatnich latach obserwuje się znaczący wzrost liczby ataków cybernetycznych. Naturalną odpowiedzią na taką sytuację jest rozwój systemów zabezpieczeń. Oprócz systemów IDS[1] oraz IPS[2] znaczenie mają również metody zwiększające świadomość sytuacyjną. Umożliwiają to m.in. systemy interaktywnych pułapek sieciowych, tzw. honeypoty. Ich działanie polega na wystawieniu na atak usług przypominających te działające produkcyjnie. Zawierają one typowe podatności, są jednak zabezpieczone przed niepożądanym wykorzystaniem i wyposażone w funkcjonalności umożliwiające rejestrowanie i raportowanie połączeń.

Istnieją dwa główne warianty pułapek sieciowych. W pierwszym są one dostępne z internetu. Należy wtedy liczyć się z dużą liczbą rejestrowanych połączeń. Zgromadzone dane pozwalają poznać metody ataku i istotne podatności. Może to być podstawą zarówno do zmiany konfiguracji urządzeń, jak i automatycznego generowania reguł filtracji dla zapór ogniowych czy sygnatur dla systemów IPS/IDS. W przypadku umieszczenia honeypota w sieci instytucji ataki powinny zdarzać się rzadko i pochodzić z wewnątrz. Zastosowanie to jest bliskie systemowi IDS, który, co jest najważniejszą różnicą, nie analizuje ruchu produkcyjnego, lecz sprowokowane połączenia. Objętość tak gromadzonych danych będzie niewielka, ale ich waga jest zdecydowanie istotniejsza. Mogą one wskazywać na nieprawidłowości w infrastrukturze, a także w ogólnej polityce bezpieczeństwa (np. dopuszczaniu osób nieuprawnionych do wrażliwych systemów).

W obu przypadkach korzyść zależy od użytych metod analizy danych, przy czym ważną rolę odgrywa automatyczna agregacji i wydajna, atrakcyjna prezentacja wyników. Żeby uzmysłowić skalę zagadnienia, wystarczy wspomnieć, że opisywany system był wyposażony w trzy pułapki sieciowe i rejestrował średnio około kilka tysięcy zdarzeń dziennie. Z tego powodu w niniejszym artykule oprócz ogólnej prezentacji prototypu systemu skupiono się na algorytmie wyszukującym podobnych sekwencji poleceń w zarejestrowanych sesjach ssh. Algorytm ten należy traktować przede wszystkim jako metodę agregacji sesji pozwalającą na ich wydajne przeszukiwanie. Należy podkreślić,

1 IDS – Intrusion Detection System – system wykrywający atak na systemy teleinformatyczne.

2 IPS – Intrusion Prevention System – system zapobiegający atakowi na systemy teleinformatyczne.

że dla honeypotów waga specyficznych fragmentów skryptu, np. adresów IP, jest mniejsza niż w przypadku IDS. W omawianym przypadku istotniejsze jest wskazanie ogólnych cech ataku, co może prowadzić do określenia jego sygnatury. Nie oznacza to oczywiście rezygnacji z obserwowania tych szczegółów. W opisywanym systemie zaproponowano w tym celu inne analizy, np. sieć powiązań między adresami IP.

Definicja zadania i sposobu jego rozwiązania

Rozważanym w artykule zagadnieniem jest wyszukiwanie podobieństw w sesjach ssh zarejestrowanych przez pułapkę sieciową cowrie[3]. Jak zauważono w trakcie eksperymentów, sesje często różnią się nieznacznymi fragmentami, np. adresami IP użytymi jako parametry poleceń systemu. Potwierdzają to także inne prace[4]. Oznacza to, że są one zazwyczaj wynikiem użycia tej samej metody ataku. Stąd propozycja narzędzia umożliwiającego wygodne wyszukiwanie sesji, dokonującego generalizacji poprzez pomijanie argumentów i wstępną klasyfikację poleceń w zależności od ich funkcji. Oryginalnym wkładem jest wykorzystanie drzew sufiksowych do wyszukiwania wspólnych podciągów w analizowanym zbiorze sesji, a także autorski algorytm redukcji zawierających się podciągów i wykorzystanie ich do wyszukiwania i prezentacji sesji. Zaletą jest brak fazy uczenia, a co za tym idzie, potrzeby przygotowania zbioru uczącego. Pozwala to na grupowanie nowych, nieobserwowanych wcześniej ataków.

Analiza danych z honeypotów

Pułapki sieciowe wymagają analizowania tysięcy zdarzeń dziennie[5]. Co istotne, można spodziewać się, że wiele z nich będzie zawierało powtarzające się informacje takie, jak: źródłowe adresy IP, użyte loginy i hasła, charakterystyczne

3 https://github.com/cowrie/cowrie [dostęp: 7.01.2023].

4 J.M. Jorquera Valero, M. Pérez, A. Huertas, G. Martinez Perez, *Identification and classification of cyber threats through SSH honeypot systems* [w:] B.B. Gupta, S. Srinivasagopalan, *Handbook of Research on Intrusion Detection Systems*, Hershey, PA 2020; O. Navarro Ferrer, *Analysis of reinforcement learning techniques applied to honeypot systems*, Master's thesis, Universitat Oberta de Catalunya, Barcelona 2021.

5 P. Rabadia, C. Valli, A. Ibrahim, Z. Baig, *Analysis of attempted intrusions: intelligence gathered from ssh honeypots* [w:] *The 15th Australian Digital Forensics Conference*, Perth 2017.

komendy czy pobierane pliki[6]. Przykładami analizatorów dla pułapki sieciowej cowrie mogą być dostępne na licencji open-source pakiety analyze-cowrie-log[7] czy cowrie-log-analyzer[8] gromadzące hasła i wyznaczające podstawowe statystyki, a także realizujące geolokalizację, wyszukiwanie pojedynczych komend czy analizę czasu trwania połączeń. Stosunkowo rozbudowany system t-pot[9] zawiera atrakcyjny wizualnie interfejs wykorzystujący pakiet Kibana[10]. Jego istotną funkcjonalnością jest przeszukiwanie danych z pomocą Elasticsearch[11]. Przykładowe analizy to geolokalizacja i rozpoznawanie systemu operacyjnego, z którego przeprowadzono atak[12], lub wyznaczanie statystyki popularności loginów i haseł[13].

Nieco bardziej zaawansowanym zastosowaniem może być generowanie sygnatur ataku typu brute-force na podstawie częstotliwości połączeń[14]. Jednakże statystyki nie mówią wiele o naturze zdarzeń czy poziomie zagrożenia. Pomagają tutaj metody klasyfikacji, wśród których można wyróżnić dwie najważniejsze grupy. Pierwsza wykorzystuje cechy połączenia raportowane przez pułapkę podobnie jak opisane wyżej statystyki. Druga skupia się na analizie sesji. Za warianty pierwszego podejścia można uznać wykorzystanie do klasyfikacji sesji maszyny wektorów podpierających (SVM)[15], a także system[16], w którym zdefiniowano 52 cechy, w tym oprócz adresu źródła czy lokalizacji geograficznej występowanie wybranych komend w sesji ssh. Należy zauważyć, że

6 K. Lasota, E. Niewiadomska-Szynkiewicz, A. Kozakiewicz, *Adaptacja rozwiązań honeypot dla sieci czujników*, „Studia Informatica" 2012, t. 33, nr 1, s. 139–148.
7 https://github.com/vwefnab/analyze-cowrie-log [dostęp: 7.01.2023].
8 https://github.com/jasonmpittman/cowrie-log-analyzer [dostęp: 7.01.2023].
9 https://github.com/telekom-security/tpotce [dostęp: 7.01.2023].
10 https://github.com/elastic/kibana [dostęp: 7.01.2023].
11 https://github.com/elastic/elasticsearch [dostęp: 7.01.2023].
12 N. Memari, S. Hashim, K. Samsudin, *Network probe patterns against a honeynet in Malaysia*, „Defence S and T Technical Bulletin" 2015, t. 8, nr 1, s. 63–75.
13 M. Boddy, *Exposed: Cyberattacks on cloud honeypots*, 2019, https://assets.sophos.com/X24WTUEQ/at/rgbjvgnx6qwwj7wvx764rmbn/sophos-exposed-cyberattacks-on-cloud-honeypots-wp.pdf [dostęp: 7.01.2023]; C. Kelly, N. Pitropakis, A. Mylonas, S. McKeown, W.J. Buchanan, *A comparative analysis of honeypots on different cloud platforms*, „Sensors" 2021, t. 21, nr 7.
14 E. Satria, T.P.S. Huda, M. Iqbal, F. Sarjana, *The investigation on cowrie honeypot logs in establishing rule signature snort* [w:] *International Conference on Agricultural Technology, Engineering, and Environmental Sciences (ICATES)*, Banda Aceh 2020.
15 J. Martinez, M. Pérez, A. Ruiz-Martínez, *A novel machine learning-based approach for the detection of ssh botnet infection*, „Future Generation Computer Systems" 2021, t. 115, s. 387–396.
16 B. Wang, J. Chen, C. Yu, *An ai-powered network threat detection system*, „IEEE Access" 2022, t. 10, s. 1–1.

wykorzystanie komend jako jednej z cech sesji zbliża tę metodę do drugiej grupy bazującej zazwyczaj na algorytmach analizy języka naturalnego. Również metoda opisana przez Febriana Setianto i współpracowników[17] jest hybrydą – używa ona algorytmu GPT2 do analizy dzienników honeypota cowrie, co jest próbą wydobycia cech przez rozpoznanie składni. System CYBEX-P[18] oprócz typowych analiz próbuje prognozować kolejne polecenie w połączeniu. Co ciekawe, prosty model wykorzystujący odległość Levenshteina daje w badanym przypadku lepsze rezultaty niż złożona sieć LSTM. Innym przykładem jest zastosowanie n-gramów do wyszukiwania podobnych sesji[19]. Reprezentacja sesji w postaci grafu[20] pozwala odwzorować powiązania komend, przy czym generalizację uzyskano dzięki pomijaniu argumentów. Kolejnym uogólnieniem jest wprowadzenie klas poleceń odpowiedzialnych za wybrane działania, np. modyfikację konfiguracji systemu czy wstępne ustalanie jego przydatności do dalszego wykorzystania[21]. Tak zdefiniowane klasy stanowią cechy wykorzystywane do klasyfikacji.

Drzewa sufiksowe

Zadanie znajdowania podobieństwa sesji można sprowadzić do wyszukiwania powtarzających się wzorców w postaci podciągów złożonych z określonej liczby znaków. W tym celu często buduje się struktury grafowe, tzw. drzewa sufiksowe (przypadek pojedynczego słowa) oraz uogólnione drzewa sufiksowe (dla zbioru słów)[22]. Metoda Ukkonena umożliwia zastosowanie wielu algorytmów, w tym znalezienie najdłuższego wspólnego podciągu czy zliczenie wszystkich wystąpień danej sekwencji.

Sposób tworzenia drzew sufiksowych przedstawia przykład z jednym słowem – „bazar" (patrz rys. 1). Budowa drzewa ma charakter inkrementalny, co

17 F. Setianto i in., *Gpt-2c: A gpt-2 parser for cowrie honeypot logs*, 2021, https://arxiv.org/abs/2109.06595 [dostęp: 7.01.2023].

18 F. Sadique, S. Sengupta, *Analysis of attacker behavior in compromised hosts during command and control* [w:] *ICC 2021 – IEEE International Conference on Communications*, Montreal 2021, s. 1–7.

19 P. Dumont, R. Meier, D. Gugelmann, V. Lenders, *Detection of malicious remote shell sessions* [w:] *2019 11th International Conference on Cyber Conflict (CyCon)*, t. 900, Tallinn 2019, s. 1–20.

20 O. Navarro Ferrer, op. cit.

21 J.M. Jorquera Valero, M. Pérez, A. Huertas, G. Martinez Perez, op. cit.

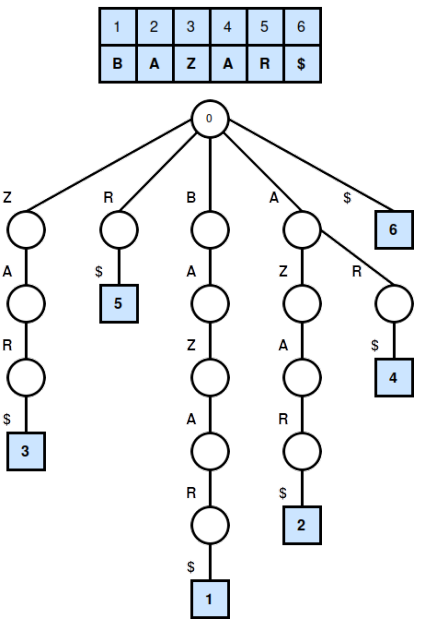
22 E. Ukkonen, *On-line construction of suffix trees*, „Algorithmica" 1995, t. 14, nr 3, s. 249–260.

pozwala na zachowanie liniowej złożoności obliczeń. W pierwszym kroku do słowa należy dodać znak niewystępujący w alfabecie np. *$* symbolizujący koniec – w podanym przykładzie *bazar$*. Punktem startowym grafu jest *korzeń* (ang. root) z indeksem 0. W każdej z n+1 iteracji należy wybrać kolejną literę (w przykładzie *b*, *ba*, *baz*, ...) i rozbudować drzewo z poprzedniej iteracji według reguł:

1) jeżeli i-ta ścieżka od korzenia kończy się *liściem* (ang. leaf node) – i-ty znak jest ostatnim elementem podciągu – to nowy znak i+1 należy dodać na końcu;

2) jeżeli i-ta ścieżka od korzenia jest zakończona *węzłem pośrednim* (istnieje kontynuacja ścieżki) i kolejne znaki są różne od nowego znaku i+1, to należy utworzyć nowe rozgałęzienie i-tego węzła, którego końcem będzie znak i+1;

3) jeżeli i-ta ścieżka od korzenia jest zakończona *węzłem pośrednim*, ale kolejny znak jest taki sam jak nowy znak i+1, to należy przejść do kolejnej iteracji.

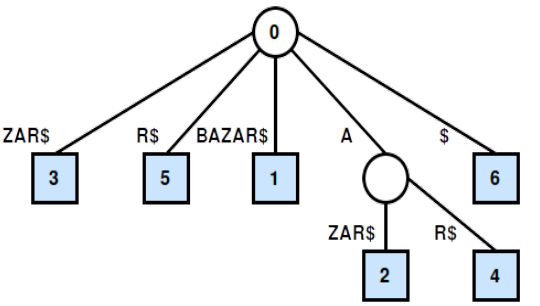


Źródło: Opracowanie własne.

Rys. 1. Konstrukcja drzewa sufiksowego dla słowa „bazar"

Ostatnim etapem jest upraszczanie struktury, rozpoczynając od końcówek. Jeżeli dany *liść* jest jedyną kontynuacją *rodzica* (nie ma więcej rozgałęzień), to węzły te można połączyć, pamiętając o aktualizacji etykiety krawędzi.

Operację należy powtórzyć dla wszystkich końcówek grafu. Końcową postać drzewa sufiksowego przedstawia rysunek 2. Liczby umieszczone w błękitnych kwadratach odpowiadają indeksowi litery, od której rozpoczyna się każda gałąź. Przedstawioną metodę można uogólnić do zadania budowy drzewa sufiksowego dla zestawu słów.



Źródło: Opracowanie własne.

Rys. 2. Końcowa postać drzewa sufiksowego

Struktura systemu

W strukturze prototypowego systemu można wyróżnić trzy warstwy:

1) pułapek sieciowych;
2) zbierania i dystrybucji danych;
3) analizy i prezentacji danych.

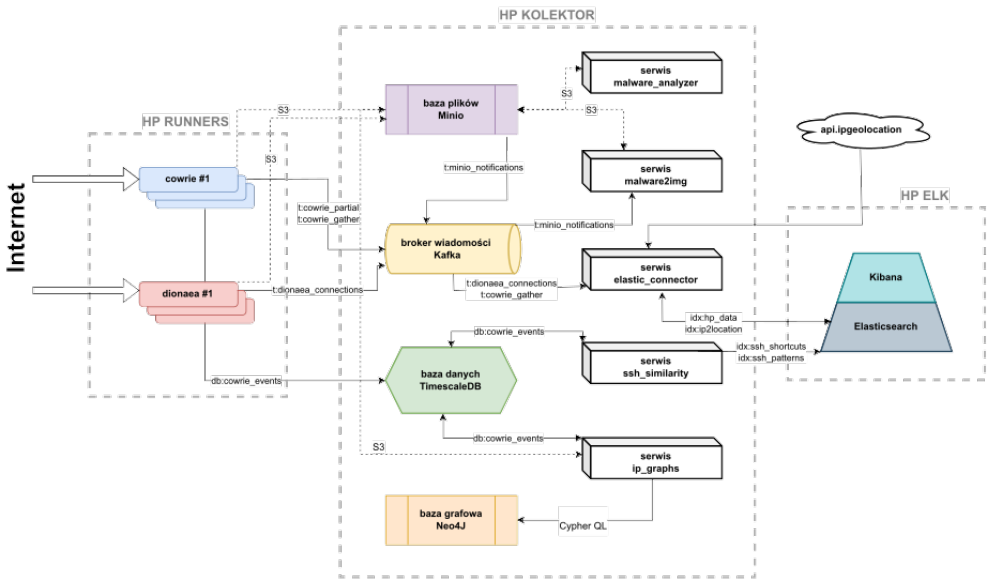
W pierwszej warstwie znajdują się pułapki sieciowe (honeypoty). W obecnej wersji wykorzystywane są dwa typy – cowrie emulujący protokół ssh oraz dionaea[23] odwzorowująca m.in. ftp, SMB, mysql, mssql, MongoDB, memcache. W warstwie zbierania i dystrybucji danych wykorzystano: broker Kafka do zbierania i udostępniania rejestrowanych zdarzeń, bazę plikową MinioDB do przechowywania przechwyconych złośliwych plików (malware), a także wyników wykonanych na nich analiz oraz bazę TimescaleDB[24] dla próbek dotyczących zarejestrowanych sesji. Dodatkowo użyto bazy grafowej Neo4J[25] do przechowywania sieci powiązań między adresami IP i URL oraz Elasticsearch,

23 *Welcome to dionaea's documentation!*, https://dionaea.readthedocs.io/en/latest/ [dostęp: 7.01.2023].
24 https://www.timescale.com/ [dostęp: 7.01.2023].
25 https://neo4j.com/ [dostęp: 7.01.2023].

którego funkcją jest filtrowanie i agregacja danych dotyczących logowań do pułapek, poleceń i skrótów sesji ssh. Analizatory danych obejmują:

1) analizator złośliwych plików: malware_analyzer i malware2img;
2) analizator danych logowania wykonujący ekstrakcję poleceń ssh i geolokalizację elastic_connector;
3) tworzenie sieci powiązań między adresami – ip_graphs;
4) wyszukiwanie podobieństw w sesjach ssh – ssh_similarity.

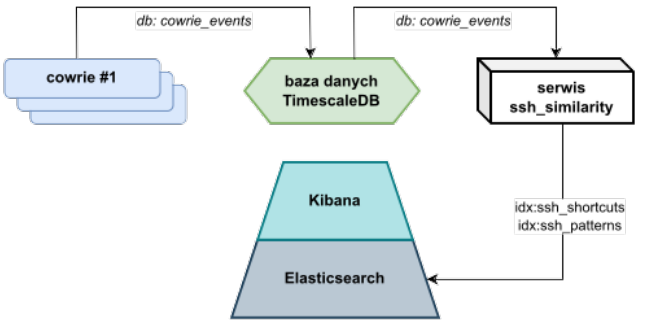
Prezentacja danych wykonana jest z pomocą narzędzia Kibana, które w połączeniu z Elasticsearch umożliwia efektywne przeszukiwanie danych. Schemat systemu przedstawia rysunek 3.



Źródło: Opracowanie własne.

Rys. 3. Schemat prototypu systemu

W dalszej części artykułu skupiono się na zaproponowanym sposobie analizy i prezentacji rejestrowanych przez system sesji ssh. Zbudowanie odpowiedniego narzędzia zmniejszającego nakład pracy operatora systemu umożliwia oddzielenie przypadków typowych, względnie będących ich niewielką modyfikacją, od szczególnie ciekawych i potencjalnie niebezpiecznych wariantów nowych, występujących pojedynczo. Schemat podsystemu przedstawia rysunek 4.



Źródło: Opracowanie własne.

Rys. 4. Schemat przepływu danych usługi ssh_similarit

Honeypot cowrie

Honeypot cowrie emuluje serwer ssh. Pozwala on na stosunkowo swobodną interakcję, np. operacje na plikach czy pobieranie danych z pomocą wget i ftp. Skutki takich operacji są ograniczone tak, żeby zminimalizować możliwość uszkodzenia pułapki bądź wykorzystanie jej do kontynuacji ataku. Zapis sesji jest zarówno przechowywany w pliku dziennika, jak i udostępniany z pomocą specyficznych protokołów, w tym hpfeeds. Ograniczenia tego protokołu (m.in. brak trwałości danych) spowodowały, że zastąpiono go bezpośrednią komunikacją z bazą TimescaleDB przechowującą zapis sesji. Dodatkowym rozszerzeniem jest tzw. plugin dla brokera Kafka[26]. Publikuje on dane zawierające podsumowanie sesji ssh.

TimescaleDB

Baza TimescaleDB[27] zawiera tabelę cowrie_events gromadzącą zdarzenia z honeypotów cowrie w postaci szeregów czasowych. Oprócz elementów wspólnych dla różnych rodzajów zdarzeń (np. stempel czasowy czy identyfikator honeypota) pozostałe dane przechowywane są w strukturze słownikowej zapisywanej w formacie binarnym. Takie podejście pozwala na zawarcie kompletu informacji, z zachowaniem możliwości przeszukiwania kluczy słownika

26 https://kafka.apache.org/ [dostęp: 7.01.2023].
27 https://www.timescale.com/ [dostęp: 7.01.2023].

z wykorzystaniem rozszerzonego języka SQL. Zapis zdarzeń w formie szeregów czasowych pozwala na tworzenie zapytań SQL operujących na wskazanym przedziale czasowym czy wybranie konkretnego typu zdarzenia z 18 generowanych, m.in. logowanie czy wgranie pliku.

Poszukiwanie wzorców sesji ssh

Obserwowane sesje wykazują znaczne podobieństwa. Korzystne byłoby grupowanie albo wyszukiwanie sesji ssh, które łączy wspólny wzorzec. W tym celu zaprojektowano serwis ssh_similarity pobierający zdarzenia z bazy TimescaleDB oraz zwracający wyniki analizy do indeksów Elasticsearch (zob. rys. 4).

Algorytm działania sprowadza się do połączenia raportowanych przez pułapkę zdarzeń w spójny zapis sesji, a następnie redukcji do skrótu literowego. Do rozpoznawania składni interpretera bash wykorzystano analizator shlex[28] wykonujący tokenizację i pozwalający odróżnić polecenia systemu od argumentów. Polecenia są kwalifikowane do 14 klas oznaczonych literami od A do N, wśród zaś argumentów wyróżniono:

1) ścieżki do plików: litera "z";
2) opcje poleceń: litera „x";
3) adresy URL: litera „y";
4) adresy IP: litera „v",
5) pozostałe, nierozpoznane: znak „;".

Tak powstałe skróty literowe są umieszczane w indeksie Elasticsearch. Podejście takie pozwala na uogólnienie zapisu sesji, tzn. utożsamianie sesji różniących się jedynie argumentami poleceń lub używających równoważnych poleceń. Przykładem mogą być „curl" i „wget", służące do pobierania plików. Kontekst nadawany poleceniom dzięki podziałowi na kategorie umożliwia drastyczną redukcję wymiarowości danych – przestrzeń 172 poleceń oraz nieograniczona liczba argumentów są zastępowane przez 19 znaków, przy czym informacja o kolejności poleceń jest zachowywana. Przykład tłumaczenia przedstawiono na rysunku 5. Na potrzeby analizy przygotowano słownik mapujący 172 najpopularniejsze polecenia systemu Linux na 14 kategorii:

28 https://docs.python.org/3/library/shlex.html [dostęp: 7.01.2023].

Tabela 1. Kategorie poleceń usługi ssh_similarity

Kategoria	Symbol	Przykład
Compression	A	gzip
Configuration	B	adduser
Display	C	cat
File operations	D	chmod
Help	E	man
Info	F	who
Install	G	pip
Networking	H	iptables
Programming	I	gcc
Shells	J	sh
System	K	kill
Text processing	L	sed
Transfer	M	wget
Utils	N	bc

Źródło: Opracowanie własne.

```
cd /tmp || cd /run || cd /; wget
http://109.206.241.200/Gummybins.sh; chmod 777
Gummybins.sh; sh Gummybins.sh; tftp 109.206.241.200 -c
get Gummytftp1.sh; chmod 777 Gummytftp1.sh; sh
Gummytftp1.sh; tftp -r Gummytftp2.sh -g 109.206.241.200;
chmod 777 Gummytftp2.sh; sh Gummytftp2.sh; rm -rf
Gummybins.sh Gummytftp1.sh Gummytftp2.sh; rm -rf *
```

```
DzDzDzMyD__J_Mvx__D__J_Mx_xvD__J_Dx___Dx
```

Źródło: Opracowanie własne.

Rys. 5. Przykład tłumaczenia sesji ssh
na skróty literowe – usługa ssh_similarity

Wyszukiwanie powtarzalnych wzorców w przetransformowanych sesjach ssh wykorzystuje koncepcję uogólnionych drzew sufiksowych. Danymi wejściowymi programu zaimplementowanego w języku Scala na bazie biblioteki gstlib[29] jest zestaw skrótów sesji ssh. Skrypt buduje w pierwszym kroku graf w postaci drzewa sufiksowego, a następnie znajduje wszystkie istniejące

29 G. Dubuisson Duplessis i in. *Utterance retrieval based on recurrent surface text patterns* [w:] *European Conference on Information Retrieval*, Aberdeen 2017, s. 199–211.

wspólne podciągi znaków oraz ich liczebność rozumianą jako liczba słów z zestawu zawierająca dany wzorzec. Wygenerowany zestaw jest następnie redukowany, ponieważ część wzorców zawiera się w pozostałych. Ignorowane są także wzorce złożone z pojedynczego znaku. Procedurę zilustrowano na abstrakcyjnym przykładzie zestawu słów „mango, banan, ananas":

1) budowa drzewa sufiksowego dla wybranego zestawu;

2) wygenerowanie listy wszystkich wspólnych podciągów – [(‚A', 3), (‚N', 3), (‚AN', 3), (‚NA', 2), (‚ANA', 2), (‚NAN', 2), (‚ANAN', 2)];

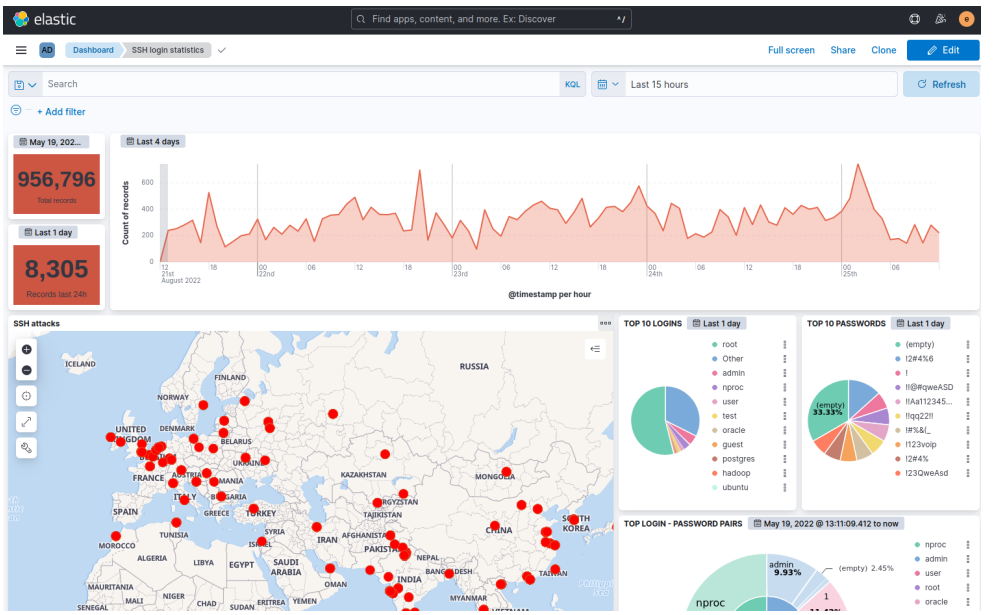
3) eliminacja wzorców o długości jednego znaku – [(‚AN', 3), (‚NA', 2), (‚ANA', 2), (‚NAN', 2), (‚ANAN', 2)];

4) eliminacja wzorców zawartych w innych wzorcach tylko wtedy, kiedy ich liczebność jest równa – [(‚AN', 3), (‚ANAN', 2)].

Odfiltrowane wzorce są zapisywane w Elasticsearch razem z częstotliwością występowania. Dzięki silnikowi wyszukiwarki możliwe jest znalezienie wszystkich sesji ssh pasujących do wykrytych sekwencji.

Elasticsearch i Kibana

Platformę Elasticsearch wykorzystano do indeksowania i wyszukiwania danych. Wbudowane mechanizmy dają wiele możliwości w zakresie przeszukiwania tekstu, filtrowania, agregacji danych i tworzenia statystyk. Elasticsearch pozwala na rozróżnienie kilkunastu typów danych, w tym stempli czasowych, adresów czy różnych formatów zapisu liczb. Szczególnie wykorzystanie formatu text pozwala na efektywne wyszukiwanie przez częściowe dopasowanie frazy, format keyword zaś na zwracanie jedynie wyników pełnego dopasowania oraz tworzenie agregacji i statystyk. Do wizualizacji danych użyto narzędzia Kibana. Jest to aplikacja webowa, która oprócz możliwości wygodnego przeglądania danych udostępnia wiele możliwości administrowania platformą, instalację dodatków, a przede wszystkim tworzenie interaktywnych ekranów (tzw. dashboardów) z wykresami. Przykładowy widok zaprezentowano na rysunku 6.

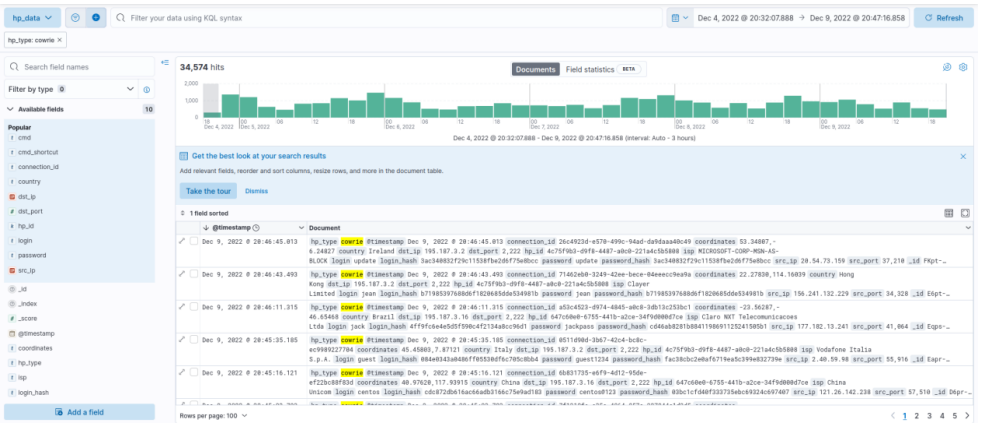


Źródło: Opracowanie własne.

Rys. 6. Przykładowy widok interfejsu graficznego przedstawiający statystyki logowań do honeypotów

Przykładowe wyniki

W celu zademonstrowania możliwości wykorzystania opisanej metody analizy sesji ssh posłużono się danymi zebranymi między 4 a 9 grudnia 2022 roku. Omawiany okres zawiera dni powszednie od poniedziałku do piątku. W tym czasie zarejestrowano 4923 sesje ssh. Na rysunku 7 przedstawiono interfejs graficzny prototypu. Widoczne są wszystkie zdarzenia zarejestrowane w omawianym okresie, w tym m.in. nieudane próby logowania, dlatego ich liczba (ponad 34 tys.) jest znacznie większa niż liczba sesji. Można zauważyć, że natężenie zdarzeń jest stosunkowo duże, rzędu kilkuset na godzinę, przy czym w godzinach nocnych daje się zaobserwować niewielki wzrost aktywności.

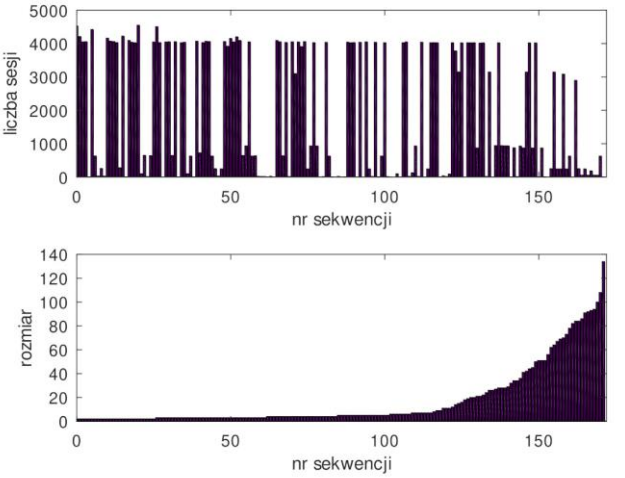


Źródło: Opracowanie własne.

Rys. 7. Widok interfejsu graficznego w trybie przeglądania zdarzeń, w górnym oknie wykres częstotliwości zdarzeń w badanym przedziale czasu

Po przetworzeniu 4923 zapisanych sesji uzyskano 172 sekwencje skrótów. Liczba ta jest stosunkowo mała, co świadczy o wydajnym działaniu procedury redukcji, może również być wynikiem małego zróżnicowania ataków, co było obserwowane podczas przeglądania danych. Dane przedstawione na rysunku 7, mimo że nie dotyczą bezpośrednio sesji, potwierdzają powtarzanie przez atakujących tych samych procedur. Widoczne są tam uporczywe próby ataku słownikowego, co ciekawe, wykonywane z wielu adresów źródłowych. W wyniku zastosowania redukcji skrótów uzyskano dość znamienny rozkład ich długości – znaczną liczbę sekwencji krótkich, które gwałtownie przechodzą w sekwencje dość długie, rzędu 100 lub więcej symboli (zob. rys. 8).

Zgodnie z oczekiwaniem wiele sekwencji krótkich odznacza się bardzo dużą liczbą dopasowań do sesji, przekraczającą często tysiąc. W większości przypadków oznacza to, że zawierają mało znaczące, powszechnie używane (często wielokrotnie w sesji) ciągi poleceń. Przykładem może być występująca w zbiorze 4038 razy sekwencja „Cz_L__Lx", która może odpowiadać poleceniom „cat /proc/cpuinfo | grep name | wc -l", ale również „cat /proc/cpuinfo | grep name | head -n}". Widoczna tu jest istotna właściwość zaproponowanej metody – kodowanie z pomocą słownika złożonego z kilkunastu symboli nie jest jednoznaczne, jednej sekwencji symboli może odpowiadać wiele sekwencji poleceń. Jak widać, podejście takie pozwala na uogólnianie znaczenia zapisu sesji – przytoczone powyżej przykłady mają podobny sens, sprowadzają się do poszukiwania informacji w pewnym pliku – wskazuje to przede wszystkim sekwencja „Cz".



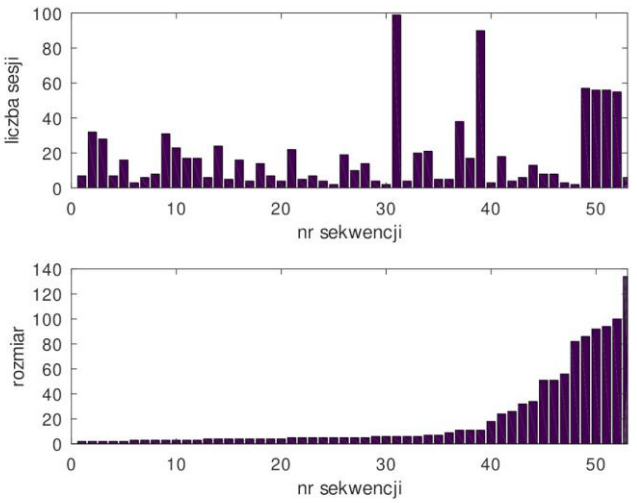
Źródło: Opracowanie własne.

Rys. 8. Liczba dopasowań sesji do kolejnych sekwencji skrótów (wykres górny) oraz długość sekwencji (wykres dolny)

O wiele bardziej symptomatyczne jest wielokrotne występowanie sekwencji długich, np. sekwencja „Cz_L__LxC__B_Jcz_L__Cx__I_Fx_L__I_DxKDKDBxF-FxCz_L__L__LxKFFxF_L_D_Dx__D__C___Dx___D" o numerze porządkowym 162 występuje w zbiorze sesji 2897 razy. Oznacza to, że analizowane sesje są rzeczywiście bardzo podobne do siebie. Przykładowe sesje odpowiadające podanemu skrótowi mogą zawierać następujące polecenia: „cat /proc/cpuinfo | grep name | wc -l echo „root:weQcvQXFk4Rn" | chpasswd"[30] lub „cat /proc/cpuinfo | grep name | wc -l echo „root:gspt2HdIhFWy" | chpasswd"[31]. Jak widać, znowu udało się dokonać generalizacji – obie przytoczone sesje zawierają próbę zmiany hasła administratora systemu. Zostało to wychwycone, mimo że podane hasła są całkowicie różne.

Żeby przyjrzeć się sekwencjom występującym rzadziej, wynikowy zbiór przefiltrowano, ograniczając się do tych, które uzyskały nie więcej niż 100 dopasowań (patrz rys. 9).

30 Zapis skrócono, aby nie zaciemniać tekstu.
31 Tak jak w poprzednim przypadku podano tylko początkowy fragment, ciąg dalszy jest identyczny w obu przypadkach.



Źródło: Opracowanie własne.

Rys. 9. Mniej popularne sekwencje – wykres górny przedstawia liczbę dopasowań sesji, wykres dolny – długość sekwencji. Ograniczono się do sekwencji z nie więcej niż 100 dopasowaniami

Na pierwszy plan wybijają się dwie sekwencje o największej liczbie dopasowań. Pierwsza z nich – „Fxxxxx", pasująca do 99 sesji, nie wydaje się szczególnie ciekawa, odpowiada wywołaniu pojedynczej komendy „uname -s -v -n -r -m". Polecenie to samo w sobie nie jest szczególnie groźne, służy bowiem do sprawdzenia wersji systemu operacyjnego oraz architektury komputera, może jednak być użyte do wstępnego rozpoznania celu, w który ma być wymierzony atak. Druga sekwencja jest nieco dłuższa: „FxB__B__Cz" i odpowiada zapisowi sesji: „uname -a; sudo hive-passwd set 234tg3ji24hj34hju345huj; sudo hive-passwd ij24ghji34hij53ji45h; cat /hive-config/rig.conf". Występuje ona w badanym zbiorze 90 razy, co jest o tyle ciekawe, że zawiera prawdopodobnie próbę przejęcia kontroli nad specyficznym systemem klastrowym przeznaczonym do obliczeń z dziedziny sztucznej inteligencji[32].

Jeżeli chodzi o sekwencje występujące najrzadziej, to można wskazać np. następującą: „C_D___". Mimo niewielkiej długości została ona zarejestrowana tylko dwa razy i odpowiada instrukcjom „cat > au; chmod +x au; ./au &". Podany przykład ilustruje zdolność algorytmu do wykrywania sesji zawierających

32 https://hiveon.com/os/ [dostęp: 7.01.2023].

nietypowe operacje. W istocie, wydaje się, że właśnie rzadko występujące skróty powinny być sprawdzane w pierwszej kolejności, potencjalnie bowiem zawierają nieobserwowane wcześniej i potencjalnie niebezpieczne połączenia.

Zakończenie

W artykule został przedstawiony prototyp systemu zbierającego i analizującego dane z pułapek sieciowych, a w szczególności jego część zajmująca się analizą i prezentacją sesji ssh zarejestrowanych przez honeypot cowrie. Zaprezentowane wyniki wskazują na użyteczność zaproponowanej metody bazującej na kodowaniu poleceń systemu operacyjnego w postaci symboli literowych i wyszukiwaniu wspólnych podciągów z użyciem drzew sufiksowych. Zastosowanie zaproponowanego algorytmu redukcji pozwala zmniejszyć liczbę podciągów do związanych ze znacząco różnymi sesjami. Należy podkreślić, że wynikowa liczba uzyskanych w ten sposób skrótów jest znacznie mniejsza niż liczba zarejestrowanych sesji. Pozwala to traktować tak uzyskany wynik jako rodzaj grupowania przeprowadzanego bez nadzoru. Co ważne, metoda ta nie wymaga zbioru uczącego oraz wstępnego określenia liczby poszukiwanych klas. Pozwala to znajdować sesje występujące rzadko czy wręcz rejestrowane pierwszy raz od uruchomienia systemu. Podczas dalszego ulepszania prototypu przewidywane jest poprawienie wygody wyszukiwania wzorców poprzez implementację graficznego narzędzia zastępującego dotychczasowy interfejs wyszukiwania Elasticsearch, a także silniejsze powiązanie z wynikami dostarczanymi przez pozostałe analizatory.

Bibliografia

Boddy M., *Exposed: Cyberattacks on cloud honeypots*, 2019, https://assets.sophos.com /X24WTUEQ/at/rgbjvgnx6qwwj7wvx764rmbn/sophos-exposed-cyberattacks-on-cloud-honeypots-wp.pdf [dostęp: 7.01.2023].

Dubuisson Duplessis G. i in., *Utterance retrieval based on recurrent surface text patterns* [w:] *European Conference on Information Retrieval*, Aberdeen 2017.

Dumont P., Meier R., Gugelmann D., Lenders V., *Detection of malicious remote shell sessions* [w:] *2019 11th International Conference on Cyber Conflict*, t. 900, Tallinn 2019.

Jorquera Valero J.M., Pérez M., Huertas A., Martinez Perez G., *Identification and classification of cyber threats through SSH honeypot systems* [w:] Gupta B.B., Srinivasagopalan S., *Handbook of Research on Intrusion Detection Systems*, Hershey, PA 2020.

Kelly C., Pitropakis N., Mylonas A., McKeown S., Buchanan W.J., *A comparative analysis of honeypots on different cloud platforms*, „Sensors" 2021, t. 21, nr 7.

Lasota K., Niewiadomska-Szynkiewicz E., Kozakiewicz A., *Adaptacja rozwiązań honeypot dla sieci czujników*, „Studia Informatica" 2012, t. 33, nr 1.

Martinez J., Pérez M., Ruiz-Martínez A., *A novel machine learning-based approach for the detection of ssh botnet infection*, „Future Generation Computer Systems" 2021, t. 115.
Memari N., Hashim S., Samsudin K., *Network probe patterns against a honeynet in Malaysia*, „Defence S and T Technical Bulletin" 2015, t. 8, nr 1.
Navarro Ferrer O., *Analysis of reinforcement learning techniquesapplied to honeypot systems*," Master's thesis, Universitat Oberta de Catalunya, Barcelona 2021.
Rabadia P., Valli C., Ibrahim A., Baig Z., *Analysis of attempted intrusions: intelligence gathered from ssh honeypots* [w:] *The 15th Australian Digital Forensics Conference*, Perth 2017.
Sadique F., Sengupta S., *Analysis of attacker behavior in compromised hosts during command and control* [w:] *ICC 2021 – IEEE International Conference on Communications*, Montreal 2021.
Satria E., Huda T.P.S., Iqbal M., Sarjana F., *The investigation on cowrie honeypot logs in establishing rule signature snort* [w:] *International Conference on Agricultural Technology, Engineering, and Environmental Sciences (ICATES)*, Banda Aceh 2020.
Setianto F. i in., *Gpt-2c: A gpt-2 parser for cowrie honeypot logs*, 2021, https://arxiv.org/abs/2109.06595 [dostęp: 7.01.2023].
Ukkonen E., *On-line construction of suffix trees*, „Algorithmica" 1995, t. 14, nr 3.
Wang B., Chen J., Yu C., *An ai-powered network threat detection system*, „IEEE Access" 2022, t. 10.

Application of suffix trees to efficient presentation of honeypot registered sessions

Abstract

The article presents a prototype of a system for analyzing data from a honeypot network. A special attention is paid to finding similarities in the collected ssh sessions. The algorithm proposed looks for generalized patterns in the session using suffix trees. The patterns can be used for a convenient presentation of the displayed sessions and for searching. The examples of analysis carried out with the help of the algorithm are presented.

Key words: honeypots, malware, session analysis, suffix trees