Protection of Critical Infrastructure in Cyberspace

MONIKA NOWIKOWSKA

Abstract Critical infrastructure plays a key role in the functioning of any modern state. One of the primary tasks of the state is to ensure adequate protection, not only for the critical infrastructure itself but also for relevant information on how to ensure its security. Critical infrastructure consists of physical and cybernetic systems, such as facilities, equipment or installations. The responsibility for proper functioning of critical infrastructure rests with state authorities and with the administrators of selected facilities, installations or equipment or services. As a result of events being the consequence of human activity or natural forces, critical infrastructure may be destroyed, damaged or disrupted, thus putting at risk the life and property of citizens. Such events have a negative impact on the economic development of the state. Hence, the protection of critical infrastructure is one of the priorities of every state. The essence of the tasks associated with critical infrastructure lies not only in ensuring its protection against risks, but also in ensuring that any possible damage or disruption to its functioning is as short-lived as possible, easy to eliminate, and does not cause additional losses to the citizens and the economy.

Keywords: • critical infrastructure • cybersecurity • public administration • critical services • critical service operator

CORRESPONDENCE ADDRESS: Monika Nowikowska, Ph.D., War Studies University, Department of New Technologies Law and Cybersecurity, Institute of Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: m.nowikowska@akademia.mil.pl, ORCID: 0000-0001-5166-8375.

https://doi.org/10.4335/2022.1.8 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

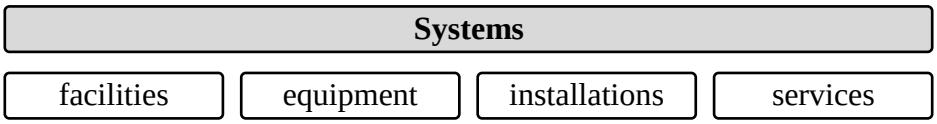
Critical infrastructure – which provides fundamental services such as the supply of energy, energy resources and fuels, communications, ICT networks, food and water – plays a key role in the functioning of a modern state. Hence, one of the primary tasks of the state is to ensure adequate protection, not only for the critical infrastructure itself but also for relevant information on how to guarantee its security (Kowalska, 2021: 645). It should be emphasised that the basic constitutional values include the internal security of the state and its citizens, which is considered an element of public order in the state. Threats to state security can be both of an external and internal nature. This means that among the tasks that state authorities undertake is to maintain the relations and processes within the state that ensure that the interests of the state and its citizens are pursued effectively and harmoniously, while simultaneously diagnosing and responding to emerging threats against these interests (Długosz, 2019: 108). This is especially relevant with regard to the smooth functioning of critical infrastructure. The responsibility for proper functioning of critical infrastructure rests with the cooperation between state authorities and the administrators of selected facilities, installations or equipment or services.

The subject matter of this paper is the protection of critical infrastructure in cyberspace. These issues raised herein required an analysis of the content and assessment of the source literature (the use of desk research) and of the selected Polish legal acts, covering three major questions: the term 'critical infrastructure', the term 'cyberspace' and the *ratio legis of* establishing special protection for critical infrastructure in cyberspace. An in-depth study of the source literature allowed the formulation of a general research problem in the form of the question: What impact does the protection have on the status of equipment, facilities and services classified as critical infrastructure? Providing an answer to this question was intended to facilitate the achievement of the research objective, i.e. the broadening and systematisation of knowledge on critical infrastructure protection in cyberspace. Due to the complexity of the general problem, it was deemed advisable to indicate in detail research problems such as: 1) types of critical infrastructure protection in cyberspace; 2) the role of the cooperation of critical infrastructure operators with each other and with the public administration in the undisturbed functioning of critical infrastructure; and 3) the functioning of the National Critical Infrastructure Protection Programme.

2 The terms 'critical infrastructure' and 'cyberspace'

The term 'critical infrastructure' has been defined in the Act of 26 April 2007 on Crisis Management (consolidated text, Polish Journal of Laws of 2020, item 1856, as amended) -hereinafter referred to as the ACM. Pursuant to Article 3(2) of the ACM, critical infrastructure shall be construed as systems and their functionally related facilities, including civil structures, equipment, installations, services essential to the security of the state and its citizens, that are required to ensure the smooth functioning of public

administration bodies, as well as institutions and entrepreneurs. Critical infrastructure applies to the supply of energy, energy raw materials and fuels, communications, ICT networks, financial services, the provision of food and potable water, the protection of health, movement of goods and people, rescue, ensuring continual effective functioning of the public administration, production, storage, warehousing and safe use and movement of chemicals and radioactive materials, including pipelines containing hazardous substances. The source literature aptly indicates that critical infrastructure consists of "those physical and cyber-based systems essential to the minimum operations of the economy and government" (Nowak, 2018: 173). The statutory definition of critical infrastructure implies that facilities, equipment, installations and services are within the framework of the aforementioned technical and social infrastructure systems, which are of high importance for the state and the society.



In Article 3 (2a) of the ACM, the legislator has also defined the term 'European Critical Infrastructure'. European Critical Infrastructure means systems and their functionally connected facilities, including civil structures, equipment and installations essential for the security of the state and its citizens and serving to ensure the smooth functioning of public administration bodies, as well as institutions and entrepreneurs, in the context of electricity, oil and natural gas, as well as road, rail, air, inland waterways transport and ocean and short-sea shipping and ports that are located in Member states, the disruption or destruction of which would have a significant impact on at least two Member states.

In analysing the term 'critical infrastructure', it is important to bear in mind that the infrastructure in question does not function in a closed space and is not isolated from the environment, but is closely interconnected with the overall ICT environment. This makes the administration and business interdependent. There is, hence, a common infrastructure that implements processes for both sectors. This leads to such degree of dependence that a malfunction of this infrastructure may produce effects beyond the borders of the organisation that manages it. It is therefore necessary to consider critical infrastructure protection as a process aimed at protecting the continuity of a particular service and its restoration if needed. Thus, critical infrastructure protection consists in undertaking all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter and mitigate all possible threats, risks or vulnerabilities.

It should be emphasised that in accordance with the disposition of Article 5b(7) of the ACM, the Director of the Government Centre for Security shall draw up, in cooperation with the relevant ministers, a uniform list of facilities, installations, equipment, and services forming critical infrastructure that is broken down by systems, whereby the list also distinguishes European Critical Infrastructure located in the Republic of Poland and

European Critical Infrastructure located in other Member States of the European Union which may have a significant impact on the Republic of Poland. The distinction of European Critical Infrastructure is related to the fact that there are facilities within the European Union which, when disrupted or destroyed, would lead to significant cross-border impacts (Długosz, 2019: 109).

Behind the term 'critical infrastructure' there is, in fact, a state policy which applies to ensuring national security and which consists in ensuring the functionality, continuity of operations and integrity of critical infrastructure in order to deter threats, risks or vulnerabilities and their effects, and to rapidly restore critical infrastructure in the event of failures, attacks or other events that disrupt its proper functioning. This policy translates into tasks of state authorities and, specifically, administrators (operators) of critical infrastructure. It is a policy of ensuring the resilience of critical infrastructure to: failures, terrorist attacks, acts of nature and other events, and so a policy of protecting against various threats. Simultaneously, it is a policy of improving the security of critical infrastructure facilities, equipment and services.

The concept of cyberspace is inextricably linked with the revolution in access to information being an effect of the IT revolution. In Polish law, the term appears in various acts that give an autonomous meaning to the term 'cyberspace'. For example, in Article 2(1a) of the Act of 18 April 2002 on the state of Natural Disaster (consolidated text, Polish Journal of Laws of 2017, item 1897), cyberspace is construed as the space for processing and exchanging information created by ICT systems, as defined in Article 3(3) of the Act of 17 February 2005 on Digitalisation of Operations of Entities Performing Public Tasks (consolidated text, Polish Journal of Laws of 2021, item 670), with the links between them and relations with users. The term 'cyberspace', construed as defined above, has also been repeated in the Act of 29 August 2002 on the Martial Law and on the Competences of the Commander-in-Chief of the Armed Forces and the Rules for his Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Polish Journal of Laws of 2017, item 1932) in Article 2(1b) and the Act of 21 June 2002 on the State of Emergency (consolidated text, Polish Journal of Laws of 2017, item 1928) in Article 2(1a). Thus, as it stems from this relatively broad definition, the legislator construes cyberspace not only as ICT systems, i.e. the equipment (hardware) they consist of, together with the programs (software) ensuring the performance of functions by these systems (processing, storage and transmission of computer data), but also as computer data (information) and interactions between devices and their users.

The term 'cyberspace' is also defined in the source literature. C. Banasinski points out that cyberspace is a conceptual hybrid that is an abbreviation of the phrase 'cybernetic(s) space' (Banasinski, 2018: 23). M. Lakomy emphasises that cyberspace is a global information infrastructure, an interconnectivity between people through computers and telecommunications (Lakomy, 2015: 67). Similarly, P. Levy notes that cyberspace is an information domain, a space for open communication via computers around the world (Levy, 2002: 380).

The analysis of definitions of cyberspace provided by legal commentators allows us to formulate certain elements characteristic for the cyberspace environment. They include: 1) unlimited reach; 2) the combination of information resources into huge databases; 3) no possibility to refer cyberspace to the physical dimensions of the real world (Wasilewski, 2013: 226); 4) the complexity of the phenomenon, by basing cyberspace on technical, technological and social elements (Dobrzeniecki, 2004: 21).

The need to take action to determine the standard norms, principles and values in cyberspace was indicated by the European Commission in its Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled "Cybersecurity Strategy of the European Union: an Open, Safe and Secure Cyberspace" (EU Commission Communication of 7 February 2013, JOIN, 2013), hereinafter, the 'Communication'. In this Communication, the Commission stressed that fundamental rights, democracy and the rule of law need to be protected in cyberspace.

Freedom in the online environment requires safety and security. Cyberspace should, hence, be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace, the mission of which should be to respect and protect fundamental rights online and to maintain the reliability and interoperability of the Internet. However, the private sector owns and operates significant parts of cyberspace, and so any initiative in this area has to recognise its leading role.

As a result of the digitisation process and the expansion of electronic communication services, new regulatory policy has become necessary. We are currently witnessing dramatic changes in the functioning of the global society and economy. The report "Proposed directions of development of the information society in Poland until 2020" indicates that the key area of changes in this regard, besides the political and economic aspects of economic competitiveness, will be the role of public authorities. The state will be forced to limit the scope of exercise of the governance function in favour of shaping development strategies and mechanisms, standardisation and mediation.

These revolutionary changes result primarily from the fact that, "the existing methods of exercising power and governing the state will simply be ineffective in a society in which information will become the main product". Digitalisation has become the reason for the convergence of administration, i.e. a process consisting in the creation of new, common administrative solutions in place of traditional administrative separateness. Such areas are subject to definition at the European Union level and their division is determined by new threats to national security (Chałubińska-Jentkiewicz, Nowikowska, 2020: 21).

One of the key regulatory objectives is to ensure cybersecurity, which requires actions related to maintaining the availability and integrity of networks and infrastructure, as well as the confidentiality of the information contained therein, subject to the right to privacy

and with respect for identity. Ensuring cybersecurity becomes one of the fundamental objectives of the state, and the determinant of these principles is the protection of fundamental values, which should have the same degree of protection in cyberspace as in the real world. An open and free cyberspace removes social and international barriers, allows the exchange of cultures and experiences between states, communities and individuals, enables interactions and the exchange of information, and consequently makes possible the exchange of knowledge, experience and technology.

To summarise this part of the discussion, it may be said that the general definition of security as a state of peace, harmony and undisturbed functioning has been broadened in recent years by cyberspace. In the past, having an army of thousands of people, the most advanced weapons and other military infrastructure was considered an element of ensuring state security. With the advent of computers, security has evolved into information security (Kitler, 2017: 19). It is widely believed that if a country cannot control its cyber assets, it is not secure. Attacks in cyberspace happen every day. If a country does not have secure systems in place, not only the country as a whole, but also its citizens are at risk of having their fundamental rights violated. Moreover, financial institutions that support the economy are vulnerable to data theft due to insecure cyber systems, and the infrastructure of a country may also be at risk as a result of cyber-attacks.

Attacks on information stored in a computer system may be twofold. Their purpose may be to undermine the credibility of the system or to steal information. In the first case, cyberterrorists enter their own data in the network or manipulate data records in the system. These attacks aim to disorganise the activities of the state, which is to the detriment of the whole society. These actions can target critical infrastructure, water and energy supply, telecommunications infrastructure, etc. Manipulating these systems can also lead to material damage or casualties, for example, if a train collision is caused. A cyberattack, by undermining the credibility of a system or stealing information, can, therefore, affect both national resources and information owned by the individual – the citizen (Holyst, 2011: 961).

W. Kitler points out that the information security of the state is a trans-sectoral field of national security, being a process of striving to ensure an undisrupted functioning and development of the state, including the society, in the information space, by providing free access to information and protecting, at the same time, against its adverse effects (tangible and intangible), by protecting information resources and systems against the hostile activities of other entities or the effects of natural forces and equipment malfunction, while maintaining the ability to informatively influence the behaviour and attitudes of international and national entities (Kitler, 2017: 19).

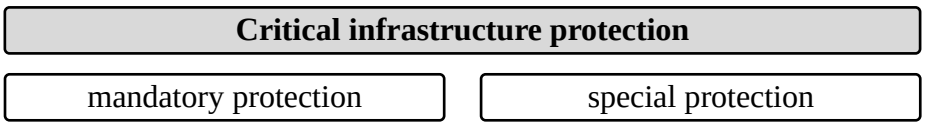
Security always applies to various manifestations of human activity. The basic attributes of security that apply to communication processes include confidentiality, which means that only authorised persons have access to certain data and information. The second element is integrity of digital content, which means that the data and information

contained therein are correct, intact and have not been manipulated. Another characteristic is availability – a rule related to the functioning of an information system, including the availability of data, processes and applications in accordance with user requirements.

3 National Critical Infrastructure Protection Programme

Critical Infrastructure Protection is defined in Article 3(3) of the ACM as all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter threats, risks or vulnerabilities, as well as to limit and neutralise their effects and to ensure their rapid restoration in case of breakdowns, attacks or other events which disrupt their proper functioning. Security in this sense can be divided into mandatory and special protection. Mandatory protection means the protection of areas, facilities, equipment and transportation systems important for the defence, economic interests of the state, public security and other important concerns of the state that is provided by specialised armed security formations or through appropriate technical safeguards, in accordance with the provisions of the Act of 22 August 1997 on the Protection of Persons and Property (Polish Journal of Laws of 2020, item 838).

Special protection, on the other hand, means the protection of facilities of particular importance for national security and defence, provided by militarised units created especially for this purpose on the basis of separate provisions. Special protection is prepared and provided under the Act of 21 November 1967 on Universal Duty to Defend the Republic of Poland (consolidated text, Polish Journal of Laws of 2021, item 372) and the Regulation of the Council of Ministers of 24 June 2003 on Facilities Particularly Important for State Security and Defence and their Special Protection (Polish Journal of Laws of 2003, No. 116, item 1090).



The principles for ensuring the security of critical infrastructure are described in the 2020 National Critical Infrastructure Protection Programme (Resolution No. 210/2015 of the Council of Ministers of 2 November 2015 on the adoption of the National Critical Infrastructure Protection Programme subject to Resolution No. 116/2020 of the Council of Ministers of 13 August 2020 amending the resolution on the adoption of the National Critical Infrastructure Protection Programme) – hereinafter referred to as the NCIPP, adopted by way of resolution of the Council of Ministers. The National Critical Infrastructure Protection Programme was initiated pursuant to Article 5b(1) of the ACM. In accordance with this regulation, the Council of Ministers adopted, by way of resolution, the National Critical Infrastructure Protection Programme, the purpose of which is to create conditions for improving the security of critical infrastructure, in

particular, with regard to: 1) preventing disruptions to the functioning of critical infrastructure; 2) preparing for crisis situations that may adversely affect critical infrastructure; 3) responding to situations of destruction of infrastructure or disruption of its functioning.

Access to critical infrastructure services is crucial for the smooth functioning and development of a modern state, society and economy. This means that a critical infrastructure that functions smoothly and without disruptions has a major impact on citizens, administrative structures and the economy. Therefore, the issue of ensuring security (protection) of critical infrastructure is very important.

The purpose of the NCIPP is to create conditions for enhancing the security of critical infrastructure. The said purpose constitutes a paramount goal of increasing the security of the Republic of Poland. In order to meet this goal it is necessary to meet a number of indirect goals, which include gaining a certain level of awareness, knowledge and competence among all actors involved in the protection process with regard to the importance of critical infrastructure for the smooth functioning of the state, as well as the ways and methods of protecting that infrastructure. Other indirect goals include: introducing a coherent risk assessment methodology that considers the whole gamut of threats, including those with very low probability and catastrophic impact; introducing a coordinated and risk assessment-based approach to performing critical infrastructure protection tasks; building a partnership between critical infrastructure protection participants; and finally, implementing the mechanisms for the exchange and protection of information shared between critical infrastructure protection participants.

According to the NCIPP, security of critical infrastructure is ensured at several levels. The tasks of critical infrastructure operators include the execution of procedures and measures to ensure physical, technical, personal and ICT security, as well as legal security. Pursuant to Article 6(1) of the ACM, the tasks of critical infrastructure protection include: 1) collecting and processing information on threats to critical infrastructure; 2) developing and enforcing procedures in the event of threats to critical infrastructure; 3) restoring critical infrastructure; 4) cooperating between public administration and owners, owner-like possessors and dependent possessors of critical infrastructure facilities, installations or equipment with respect to their protection.

The starting point for critical infrastructure protection is Article 6(5) and (5b) of the ACM, which states that owners, owner-like possessors and dependent possessors of critical infrastructure facilities, installations or equipment are obliged to protect them, in particular, by preparing and implementing, adequately to the foreseen threats, critical infrastructure protection plans and by maintaining their own backup systems, as well as ensuring security and sustaining the functioning of this infrastructure until its complete restoration.

This regulation implies a general obligation to protect critical infrastructure components regardless of the legal title to the facilities, installations or equipment that make up critical infrastructure, and so by all entities which may actually and legally affect the functioning of critical infrastructure (Długosz, 2019: 111). The Court of Appeal in Warsaw in its judgement of 10 October 2013, I ACa 767/13, emphasised that the mere fact that the Act on Crisis Management does not include any provisions imposing sanctions on those critical infrastructure managers who fail to comply with the dispositions contained in the provisions of the Act and refuse to cooperate with the public administration does not, however, indicate that actions contrary to these provisions should be considered lawful, i.e. devoid of legal sanctions under the provisions of other acts. In addition, section 5a of the ACM provides that owners, owner-like possessors and dependent possessors are obliged to designate, within 30 days of receiving information on inclusion of facilities, installations or equipment in the "list of critical infrastructure facilities, installations, equipment and services split into systems" - a person responsible for maintaining contact with competent entities within the scope of critical infrastructure protection.

Article 6(5b) of the ACM provides that operators of essential services are obliged to include, in critical infrastructure protection plans, documentation concerning the cybersecurity of the information systems used to provide essential services. Pursuant to the said regulation, owners, owner-like possessors and dependent possessors being the operators of essential services within the meaning of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Polish Journal of Laws of 2020, item 1369 as amended), hereinafter referred to as the ANCS, shall include in critical infrastructure protection plans the documentation regarding the cybersecurity of the information systems used to provide essential services, in accordance with the scope of information set out in the regulations issued pursuant to the Act on the National Cybersecurity System.

4 Cooperation of critical infrastructure operators

In the Act on Crisis Management, the legislator adopted a sanction-free approach to the protection of critical infrastructure. This is based on the assumption that the effectiveness of critical infrastructure protection can be increased only through the actions of its operators when supported by the capabilities and potential of the public administration. Critical infrastructure operators have the best knowledge and tools to mitigate threats to their activities. They are also in a position to make the most appropriate choice of strategies to minimise the impact of these threats.

The term ‘operator of essential service’ has been defined in the ANCS. Article 2(16) of the ANCS also defines the term ‘essential service’. An essential service is a service that is essential for the maintenance of critical societal and/or economic activities that are included in the list of essential services. This means that it is a necessary condition that it is a service included by the legislator in the list of essential services that constitutes Annex 1 to the Act (Czarnecka, 2019: 64). The status of an operator of essential services may be

obtained only by an entity that provides services included in this list. Another prerequisite is to have an organisational unit in the Republic of Poland. Neither the actual nature of the conducted activity nor its size is decisive. For an entity to be recognised as an operator of essential service, it is necessary for the authority responsible for cybersecurity to issue a decision recognising the given entity as an operator of essential service.

The list of essential services is annexed to the ANCS. Essential services have been specified for each sector (or sub-sector, if any). For example, within the energy sector, seven subsectors have been distinguished and listed, with the essential services relating to them: 1) mineral extraction (extraction of natural gas, oil, brown coal, hard coal, copper); 2) electric energy (generation, transmission, distribution of electric energy, trading in electric energy, storage of electric energy, systemic and quality services, management of energy infrastructure); 3) heat (generation of heat, trading in heat, transmission and distribution of heat); 4) oil (production of liquid fuels, transmission of oil, transmission of liquid fuels, storage of oil, transhipment of oil, storage of liquid fuels, transhipment of liquid fuels, trading in liquid fuels or trading in liquid fuels with foreign countries, production of synthetic fuels) 5) gas (production and transmission of fuel gases, trading in fuel gases and trading in natural gas with foreign countries, transmission, distribution, storage of fuel gases, liquefaction and regasification of LNG, as well as importing and unloading); 6) supplies and services for the energy sector (supply of systems, machinery, equipment, materials, raw materials and provision of services to the energy sector); 7) units subordinated or supervised (production of radiopharmaceuticals, management of radioactive waste, maintenance of strategic reserves and stocks of oil, petroleum products and natural gas, research and development or implementation or technological research for the energy sector) (Kitler, Taczkowska-Olszewska, Radoniewicz, 2019: 28).

In an attempt to maintain balance between the sovereign influence of the state and the expenditure necessary to improve the security of critical infrastructure, the legislator did not provide in the ACM sanctions for failure to comply with the obligations set out therein, nor for budget support for critical infrastructure operators. Therefore, in order to achieve the assumed objectives, it was necessary to adopt the rules to be followed by its participants. Namely, the pillars of cooperation are: 1) joint responsibility, construed as a collective drive to improve the security of critical infrastructure, arising from awareness of its importance for the functioning of both public administration bodies and critical infrastructure operators, society, the economy and the state; 2) cooperation, which means that participants in critical infrastructure protection perform together specific, convergent and complementary tasks in order to achieve a common goal, which results from the principle of joint responsibility; 3) trust, construed as the conviction that the motivation of the critical infrastructure protection participants is the pursuit of a common goal – improving the security of critical infrastructure.

This means that the basic method of critical infrastructure protection is the cooperation of the administrators of that infrastructure with each other and with the public

administration. It should be emphasised that in Article 6 of the ACM, the legislator did not exhaustively define the methods of critical infrastructure protection, while the disposition of Article 5b(9) of the ACM implies the obligation of public administration bodies and services responsible for national security to cooperate with owners, autonomous possessors and dependant possessors of critical infrastructure facilities, installations, equipment and services, as well as with other public authorities and services. Hence, the point is that operators should be governed by the protection of critical infrastructure insofar as their legal and factual capabilities allow. They should implement, as far as possible, measures to ensure functionality, continuity and integrity of critical infrastructure in order to deter, mitigate and neutralise threats, risks or vulnerabilities, and to recover that infrastructure rapidly in case of failures, attacks or other events that disrupt its proper functioning.

Thus, critical infrastructure protection integrates measures drawn from various areas, and mobilises critical infrastructure administrators to make best use of their capabilities in order to prepare for threats to, or to improve the security of, critical infrastructure. These capabilities also include the cooperation of critical infrastructure operators and the cooperation of these operators with public administration, which is related to this "systemic" view of critical infrastructure (Długosz, 2019: 11). This conclusion is confirmed by the content of the NCIPP, where cooperation on the protection of critical infrastructure is considered one of the most important principles to become a key element in ensuring coherence of decisions made and effectiveness of the actions taken, both in the course of day-to-day work and in situations of threats.

The main addressees of the NCIPP in the government administration are the ministers responsible for critical infrastructure systems and the heads of particular provinces, while the operators of critical infrastructure, pursuant to Article 6 of the ACM, are obliged to protect it.

5 Obligations of operators of essential services

It should be emphasised that in the ANCS, the legislator has imposed on operators of essential services (Articles 8-15 of the ANCS) over a dozen obligations relating to ensuring the smooth operation of the security management system in the information system. In the case of operators of essential services, only serious incidents are to be reported to the relevant CSIRT (Besiekierska, 2019: 65). When handling an incident, an operator of essential service is obliged to classify the incident based on the thresholds indicated in the Regulation of the Council of Ministers of 31 October 2018 on the thresholds for considering an incident as serious (Polish Journal of Laws of 2018, item 2180).

The nature of the incident may depend on the number of users affected by the disruption to the provision of the essential service, the duration of the impact of the incident on the essential service provided, the geographical extent of the area affected by the incident and

other factors specific to the sector or sub-sector concerned. The criteria for considering an incident as serious are defined separately for each of the essential services. For example, in the case of water supply, a serious incident will be an incident that led to the unavailability of the service to at least 100,000 users for more than 8 hours. In the case of an incident concerning the provision of healthcare services, it will be an incident that led to the non-availability of the service for more than 24 hours or to one or more of the following: human death; serious injury; other than serious injury to more than one person; lack of confidentiality of data processed in the service; lack of integrity of data processed by the service.

Another obligation under the ANCS is the obligation imposed on operators of essential services to establish internal structures responsible for cybersecurity. An alternative is to conclude an agreement with a provider of cybersecurity services, as provided for in the ANCS, who meets the criteria indicated in the Regulation of the Minister of Digitalisation of 10 September 2018 on Organisational and Technical Conditions for providers of cybersecurity services and internal organisational structures of operators of essential services responsible for cybersecurity (Polish Journal of Laws 2018, item 1780).

It needs to be emphasised that in the ANCS, the legislator provided for sanctions for failure to fulfil obligations. Article 73 (1) and (2) of the ANCS contains a catalogue of infringements of obligations which are subject to financial penalties. The Act does not provide for penalties in the case of public bodies. The operator of essential service may be fined up to PLN 200,000 (or up to PLN 1,000,000, if, as a result of an inspection, it turns out that there is a persistent violation of the provisions of the Act). In addition, the competent authority responsible for cybersecurity may impose a penalty payment on the manager of the essential service operator in the amount corresponding to 200% of his/her monthly salary at the maximum. This applies to the case where such a manager has failed to exercise due diligence to fulfil some of the obligations indicated in the ANCS.

6 Conclusion

Critical infrastructure protection is an ongoing and dynamic phenomenon. This is due to the fact that the perception of threats, the scope of available resources and the possibilities to protect critical infrastructure are changing. Simultaneously, critical infrastructure protection addresses various aspects of the critical infrastructure operation and integrates the means of protection from various areas, such as the provision of physical security.

Protection of critical infrastructure in cyberspace has been additionally regulated in the ANCS. Prior to the entry into force of the ANCS, the issues of securing information and communication systems were regulated by sector or in a fragmentary way. Insufficient protection of information and communication systems is related to the issue of cyberterrorism as a source of threats to critical infrastructure. The provisions of the ANCS significantly affect the identification of critical infrastructure and threats to its functioning, as well as introduce new means of protection in the cybernetic area. Among

other issues, the Act defines cybersecurity as the required functionality of critical infrastructure, and identifies operators of essential services among the most important entities conducting business in Poland.

According to the act, essential services are those which are crucial for the maintenance of critical societal and/or economic activities, and so we deal with a term that is convergent with the term 'critical infrastructure', whereby essential services explicitly include services in the following sectors: energy, transport, banking and financial market infrastructure, health care, drinking water supply and distribution, as well as what is known as digital infrastructure. The selected operators of essential services are subject to the obligation to implement information system security management systems in order to provide an essential service, which consist of a number of components, e.g. the means of communication enabling proper and secure communication within the national cybersecurity system.

These information system security management systems can be seen as a new means of critical infrastructure protection to be used by those critical infrastructure administrators or providers of the services classified as critical infrastructure, who have been considered as operators of essential services within the meaning of the ANCS. Similarly, the documentation developed by the operators of essential services on the cybersecurity of the information systems used to provide essential services will translate into the content of the critical infrastructure protection plans, thus becoming the means of critical infrastructure protection.

Various actions are taken as part of critical infrastructure protection, which aim to ensure the critical infrastructure functionality, continuity and integrity in order to deter threats, risks or vulnerabilities and to mitigate and neutralise their impact, and to recover that infrastructure rapidly in case of failures, attacks or other events that disrupt its proper functioning. Cooperation between operators within critical infrastructure systems, as well as between critical infrastructure systems plays an important role in this protection. The links between individual critical infrastructure components or facilities and the need for a comprehensive (holistic) approach necessitates the far-reaching cooperation of all the entities responsible for the undisturbed functioning of critical infrastructure. This cooperation takes place during the planning phase of critical infrastructure protection and later during its implementation. It takes the form of fairly concrete legal obligations that come with participation in the National Critical Infrastructure Protection Programme and the development of critical infrastructure protection plans.

Critical infrastructure protection is a complex task, and the way this task is carried out changes over time, among other things, due to the fact that the legal environment for the functioning of the critical infrastructure operators is changing. A good example is the ANCS, which has undoubtedly strengthened critical infrastructure protection in the cybernetic dimension.

References:

Banasiński, C. (2018) Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo. Zarys wykładu* (Warsaw: Wolters Kluwer), pp. 21-65.

Besiekierska, A. (2019) Ustawa o krajowym systemie cyberbezpieczeństwa. Wybrane obowiązki jednostek sektora finansów publicznych i spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej, *Informacja w administracji publicznej*, 1, pp. 65-69.

Chałubińska-Jentkiewicz, K. & Nowikowska, M. (2020) *Bezpieczeństwo, tożsamość, prywatność – aspekty prawne* (Warszawa: C.H. Beck).

Czarnecka, A. (2019) Wybrane obowiązki operatorów usług kluczowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa, *Informacja w administracji publicznej*, 2, pp. 64-69.

Długosz, T. (2019) Ochrona infrastruktury krytycznej przez przedsiębiorców, In: Pawłowski, A. & Wolska, K. (eds.) *Przedsiębiorcy i ich działalność* (Warszawa: C.H. Beck), pp. 108-111.

Dobrzeniecki, K. (2004) *Prawo a etos cyberprzestrzeni* (Toruń: Wydawnictwo Adam Marszałek).

Hołyst, B. (2011) *Terroryzm* (Warszawa: LexisNexis).

Kitler, W. (2017) Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne, In: Kitler, W. & Taczkowska-Olszewska, J. (eds.) *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne* (Warszawa: Wydawnictwo Towarzystwo Wiedzy Obronnej), pp. 19-28.

Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz, F. (eds.) (2019) *Ustawa o krajowym systemie cyberbezpieczeństwa*. *Komentarz* (Warszawa: C.H. Beck).

Kowalska, K. (2021) Przetwarzanie danych o karalności pracowników i kandydatów na pracowników w kontekście dostępu do informacji o bezpieczeństwie infrastruktury krytycznej, *Monitor Prawniczy*, 12, p. 645-651.

Lakomy, M. (2015) *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państwa* (Katowice: Wydawnictwo Uniwersytetu Śląskiego).

Levy, P. (2002) Drugi potop, In: Hopfinger, M. (ed.) *Nowe media w komunikacji społecznej XX w. Antologia* (Warszawa: Wydawnictwo Oficyna Naukowa), pp. 380-389.

Nowak, W. (2018) Ochrona infrastruktury krytycznej w cyberprzestrzeni, In: Banasiński, C. (ed.) *Cyberbezpieczeństwo. Zarys wykładu* (Warszawa: Wolters Kluwer), pp. 173-194.

Wasilewski, J. (2013) Zarys definicyjny „cyberprzestrzeni", *Przegląd Bezpieczeństwa Wewnętrznego*, 9, pp. 226-231.