Cybersecurity System in Poland. Selected Legal Issues

JAROSŁAW KOSTRUBIEC

Abstract The reliability of information systems currently determines the effectiveness of the state in the sphere of providing many services. These systems not only facilitate communication, but are also fundamental to public, social or economic activity. Therefore, ensuring a high level of security of information systems must be an important direction of the state policy. It is the national cybersecurity system that is expected to ensure cybersecurity in Poland, including the uninterrupted provision of essential and digital services.

Keywords: • cybersecurity • information systems • essential services

CORRESPONDENCE ADDRESS: Jarosław Kostrubiec, Ph.D., Dr. Habil., University Professor, Maria Curie-Sklodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, e-mail: jaroslaw.kostrubiec@mail.umcs.pl, ORCID: 0000-0003-1379-9846.

https://doi.org/10.4335/2022.1.1 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

In the justification of the government's draft National Cybersecurity System Act (Parliamentary Paper No. 2505, https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2505) (the Justification), the drafters clearly emphasise that due to the ever-increasing influence of information and communication technologies on the socio-economic development of the European Union Member States, as well as the increase in their use, the products and services offered are now increasingly dependent on ensuring cybersecurity. The extensive architecture of information and communication systems, including operations on large data resources, contribute to the development of communications, trade and transport and constitute the basis for the functioning of essential and digital services, as well as services provided by public administration. These form the basis for today's economy and for modern civil society (Bożek, Karpiuk, Kostrubiec & Walczuk, 2012: 200-203). It should be stressed, however, that the opportunities offered by modern digital technologies are also used for the undertaking of undesirable activities – unfair competition practices, interruptions of the continuity of selected services, committing crimes via the Internet, as well as undertaking terrorist activities.

The basic regulations on the protection of cybersecurity in the European Union are provided for in the NIS Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ EU of 2016 L 194, p. 1). As stated in Article 1 of the NIS Directive, it lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market. To that end, the NIS Directive: 1) lays down obligations for all Member States to adopt a national strategy on the security of network and information systems; 2) creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them; 3) creates a computer security incident response teams network (hereinafter referred to as "the CSIRTs network") in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation; 4) establishes security and notification requirements for operators of essential services and for digital service providers; 5) lays down obligations for Member States to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.

Security of network and information systems, as defined in Article 4 (2) of the NIS Directive, means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data, or the related services offered by, or accessible via, those network and information systems. Cybersecurity is a specialised field in security engaged, among other activity, in protecting information systems against threats (Czuryk, 2019: 42).

The Polish lawmakers, meeting the requirements of the NIS Directive, regulated cybersecurity issues in the Act of 5 July 2018 on the National Cybersecurity System (i.e. Journal of Laws of 2020, item 1369, as amended.), hereinafter referred to as the NCSA. In the NCSA, the legislator has regulated: 1) the organisation of the national cybersecurity system and the tasks and responsibilities of the entities operating within this system; 2) the exercise of supervision and control within the scope of the compliance with the provisions of the NCSA; 3) the scope of the Cybersecurity Strategy of the Republic of Poland.

2 Entities of the National Cybersecurity System

In the subjective aspect, the National Cybersecurity System (Article 4 NCSA) covers: 1) operators of essential services; 2) providers of digital services; 3) CSIRT MON; 4) CSIRT NASK; 5) CSIRT GOV; 6) selected sectoral cybersecurity teams; 7) selected public-finance entities; 8) research institutes; 9) the National Bank of Poland; 10) Bank Gospodarstwa Krajowego; 11) the Office for Technical Inspection; 12) the Polish Air Navigation Services Agency; 13) the Polish Centre for Accreditation; 14) the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management; 15) commercial companies and partnerships carrying out tasks of general interest, the aim of which is to satisfy the collective needs of the population on an ongoing and uninterrupted basis by providing generally accessible services 16) entities which provide cybersecurity services; 17) authorities in charge of cybersecurity; 18) the Single Point of Contact for cybersecurity; 19) the Government's Plenipotentiary for Cybersecurity; 20) the Cybersecurity Board. The legislators chose entities that they believed played a vital role in the cybersecurity system – and which are also important from the point of view of the strategic interests of the country, including in the field of telecommunications (Karpiuk, 2021: 237).

The backbone of the National Cybersecurity System is made up by public entities, since they set the policy direction in this area. Their status and tasks, however, differ, as does their place in the public sphere. Their common goal is to ensure security in cyberspace, construed as the space for processing and exchanging information created by communication and information systems, along with interconnections and relations with users. The legal status of public entities in the sphere of cybersecurity in Poland is determined primarily by the NCSA. It defines the organisation of the national cybersecurity system, the aim of which is to ensure cybersecurity in Poland. This also concerns the uninterrupted provision of essential services and digital services, and is accomplished by achieving an adequate level of security of the information systems used to provide these services and by ensuring the handling of incidents perceived as events that have or may have an adverse impact on cybersecurity. The legislator also defines the tasks and responsibilities of the entities operating within this system, as well as the exercise of supervision and control within the scope of the compliance with the provisions of the said act.

Cybersecurity is one of the tasks of both government administration and local self-government (Kostrubiec, 2021: 115-118), as well as of other entities entrusted with competences in this area. The lawmakers define cybersecurity as the ability of information systems to resist any action which compromises the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. Entities of the National Cybersecurity System have been obliged to protect against cybersecurity threats, hence, against the potential causes of an incident perceived as an event which has, or may have, an adverse impact on cybersecurity (K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, 2021: 1).

The NIS Directive does not regulate exhaustively the catalogue of entities that are to co-create national cybersecurity systems. It only defines the functions necessary for the interoperability of national systems that, together, form a system at a European level. Consequently, the national legislators had considerable leeway in this regard, within which it extended the participation of public entities beyond the scope necessary for the transposition of the Directive. At the same time, it should be emphasised that a simple enumeration of these entities, as well as the assignment of various powers and duties to them in subsequent chapters does not satisfy the need for a clear and functional structure of the system (Szpor, 2019a: LEX/el.).

The legislator has imposed, as part of the National Cybersecurity System, a number of obligations on public entities to ensure that information systems are resistant to actions which compromise the confidentiality, integrity, accessibility and authenticity of processed data, and the related services offered by such systems. These responsibilities include obligations to report and handle an incident in a public entity, as well as the obligation to appoint a person responsible for maintaining contact with the national cybersecurity system entities. The above obligations have not been imposed on all public entities, but have been explicitly indicated by the legislator. An important spectrum of activities in this respect concerns incidents occurring in a public entity, i.e. incidents that cause or may cause a decrease in the quality or interruption of the performance of a public task carried out by a public entity. A special place within the responsibilities of public entities is occupied by incident handling – construed as activities enabling the detection, recording, analysis, classification, prioritisation, taking corrective actions and limiting the effects of an incident (Karpiuk, 2020: 57).

3 Operators of essential services

Operators of essential services are an important element of the National Cybersecurity System. According to Article 5 NCSA, an operator of an essential service is an entity, referred to in Annex 1 to the NCSA, with an organisational unit on the territory of the Republic of Poland, for which the competent authority for cybersecurity issued a decision recognising the given entity as an operator of an essential service. The competent authority for cybersecurity shall issue a decision recognising the entity as an operator of

an essential service, if: 1) the entity provides an essential service; 2) the provision of this service depends on information systems; 3) an incident would have significant disruptive effects on the provision of essential service by that operator. Where the entity provides an essential service in other Member States of the European Union, the competent authority for cybersecurity shall, in the course of administrative proceedings, through the Single Point of Contact, consult with those states to determine whether that entity is recognised as an operator of an essential service in those states. For the entity that no longer meets the statutory requirements, the competent authority for cybersecurity shall issue a decision declaring an expiration of the decision recognising it as an operator of an essential service. Essential services cover the following sectors: 1) energy (electric energy, heat, oil and gas); 2) transport (water, land and air transport); 3) banking and financial markets infrastructure; 4) water treatment and sewage disposal; 5) health care; 6) digital infrastructure. This follows from the Appendix to the Regulation of the Council of Ministers of 11 September 2018 on the list of essential services and the thresholds of materiality of disruptive effect of an incident on the provision of essential services (Journal of Laws 2018, item 1806 as amended).

The minister competent for computerisation shall maintain the list of operators of essential services that specifies: 1) name (business name) of the operator of an essential service; 2) sector, sub-sector and type of the entity; 3) registered office and address; 4) tax identification number (NIP), if assigned; 5) number in the relevant register, if assigned; 6) name of an essential service, consistent with the list of essential services; 7) date of commencement of the provision of essential services; 8) information specifying in which Member States of the European Union the entity has been recognised as an operator of an essential service; 9) date of termination of the provision of essential services; 10) date of removal from the list of operators of essential services – Article 7 (1-2) of the NCSA.

Pursuant to Article 7 (7-8) of the NCSA, data from the list of operators of essential services are made available by the minister competent for computerisation, to CSIRT MON, CSIRT NASK and CSIRT GOV and to the sectoral cybersecurity team within the scope of the sector or subsector for which it was appointed, as well as to the operator of an essential service within the scope concerning that operator. Upon request, the data from the list of operators of essential services shall be made available by the minister competent for computerisation, to the extent necessary for the performance of statutory tasks of such operators, to the following entities: 1) competent authorities for cybersecurity; 2) the Police; 3) the Military Police; 4) the Border Guard; 5) the Central Anti-Corruption Bureau; 6) the Internal Security Agency and the Intelligence Agency; 7) the Military Counterintelligence Service and the Military Intelligence Service; 8) courts; 9) the prosecutor's office; 10) the National Fiscal Administration authorities; 11) the Director of the Government Centre for Security; 12) the State Protection Service.

An operator of an essential service, pursuant to Article 8 of the NCSA, shall implement a security management system for the information system used for the provision of an

essential service, which shall ensure: 1) regular incident-risk assessment and risk management; 2) the implementation of the appropriate technical and organisational measures proportionate to the assessed risk, taking into account the latest state of the art, including: a) the maintenance and safe operation of the information system, b) physical and environmental security, including access control, c) the security and continuity of services key to the provision of the essential service, d) the deployment, record-keeping and maintenance of action plans that allow the continuous and uninterrupted provision of the essential service, and ensure the confidentiality, integrity, availability and authenticity of information, e) the implementation of a continuous monitoring system to supervise the information system used to provide the essential service; 3) the collecting of information on cybersecurity threats and the vulnerabilities of the information system used to provide the essential service; 4) incident management; 5) the applying of measures to prevent and minimise the impact of incidents on the security of the information system used to provide the essential service, including: a) using mechanisms to ensure the confidentiality, integrity, availability and authenticity of the data processed in the information system, b) keeping the software up to date, c) security measures against unauthorised modification in the information system, d) taking immediate action on identifying a vulnerability or a cybersecurity threat; 6) using the means of communication which facilitate accurate and safe communication within the national cybersecurity system.

Pursuant to Article 9 of the NCSA, an operator of an essential service shall: 1) designate a person responsible for communicating with entities in the National Cybersecurity System; 2) provide users of essential services with access to the knowledge that allows them to understand cybersecurity threats and employ effective precautions against such threats within the scope associated with the essential services provided, in particular, by publishing relevant information on the operator's website; 3) provide the competent authority for cybersecurity with relevant data, no later than within 3 months of changing the data. An operator of an essential service shall provide the competent authority for cybersecurity (the relevant CSIRT MON, CSIRT NASK, CSIRT GOV and the sectoral cybersecurity team) with data including name, phone number and e-mail address, within 14 days of the date of appointment of the person responsible for maintaining contact with the entities of the National Cybersecurity System, as well as information on changing these data – within 14 days of the date of the change.

As provided in Article 10 of the NCSA, an operator of an essential service shall develop, apply and update the cybersecurity documentation of the information system used to provide the essential service. Such operator is required to establish oversight of the cybersecurity documentation of the information system employed to provide the essential service, ensuring that: 1) the documents shall be made available only to authorised persons, in accordance with the tasks performed by them; 2) the documents shall be protected against misuse or loss of integrity; 3) subsequent versions of the documents shall be indicated in a way making it possible to identify the changes made in such documents. An operator of an essential service shall store the cybersecurity documentation of the information system used to provide the essential service for a

minimum period of 2 years of the date of its withdrawal from use or termination of the provision of the essential service. If such operator is, at the same time, the owner, owner-like possessor or dependent possessor of facilities, installation, equipment or services being parts of critical infrastructure and has an approved critical infrastructure protection plan that includes cybersecurity documentation of the information system used to provide the essential service, such operator shall not be obliged to develop cybersecurity documentation of the information system used to provide the essential service.

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 required to ensure the smooth functioning of public administration bodies, as well as institutions and entrepreneurs. Critical infrastructure covers: 1) the supply of energy, energy-producing raw materials and fuels; 2) communications systems; 3) ICT networks; 4) financial systems; 5) food supply; 6) water supply; 7) health care systems; 8) transport systems; 9) rescue systems; 10) systems ensuring the continuity of public administration; 11) manufacturing, warehousing, storage and use of chemical and radioactive substances, including pipelines of dangerous substances. This follows from Article 3(2) of the Act of 26 April 2007 on Crisis Management (Journal of Laws of 2019, item 1398 as amended).

Cybersecurity documentation of the information system applied to provide an essential service consists of: 1) normative documentation and 2) operational documentation. Normative documentation is made up by: 1) documentation relating to the information security management system produced in accordance with the requirements set out in the standard PN-EN ISO/IEC 27001; 2) documentation relating to infrastructure protection, with the use of which the essential service is provided, concerning: (a) characteristics of the essential service and infrastructure, (b) assessment of the risk for infrastructure facilities, (c) assessment of the existing infrastructure protection (risk treatment plan), (d) description of technical protections of infrastructure facilities, (e) principles of organisation and execution of physical protection of infrastructure, (f) data on specialised armed security services that protect the infrastructure, if any (specialised armed security services are internal security services and entrepreneurs who have obtained concessions for conducting economic activity in the scope of services consisting in protecting persons and property, possessing weapon on the basis of weapon certificate, Article 2 (7) of the Act of 22 August 1997 on the Protection of Persons and Property, Journal of Laws of 2017, item 2213 as amended); 3) documentation of the essential service continuity management system produced in accordance with the requirements set out in the standard PN-EN ISO 22301; 4) technical documentation of the information system used to provide the essential service; 5) documentation resulting from the specificity of the essential service provided in a given sector or sub-sector. Normative documentation is made up by: 1) documentation relating to procedures and instructions resulting from normative documentation; 2) descriptions of the ways to document the performance of activities under the established procedures; 3) documentation certifying each time a procedure is performed (§ 1-3 of the Regulation of the Council of Ministers of 16 October 2018 on

Types of Cybersecurity Documentation of the Information System used to provide an essential service (Journal of Laws of 2018, item 2080).

Pursuant to Article 11 of the NCSA, an operator of an essential service shall: 1) ensure incident handling; 2) provide access to information on recorded incidents to the relevant CSIRT MON, CSIRT NASK, or CSIRT GOV, insofar as necessary for the performance of its tasks; 3) classify a given incident as serious based on the thresholds for recognising a given incident as serious; 4) promptly report any serious incident, not later than within 24 hours from its detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV; 5) cooperate with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV during the handling of a serious incident and critical incident, by providing the required data, including personal data; 6) remove vulnerabilities and notify the competent authority for cybersecurity of their elimination. A serious incident shall be reported electronically or, if impossible, with the use of other available means of communication. Where a sectoral cybersecurity team is appointed, an operator of an essential service shall: 1) concurrently transmit the report electronically to the team; 2) cooperate with the team at the sector or sub-sector level during the handling of a serious incident or critical incident, by providing the necessary data, including personal data; 3) provide the team with access to information on recorded incidents, insofar as necessary for the performance of its tasks. The thresholds for considering an incident as serious according to incident type, in particular, sectors and sub-sectors, are defined by the legislator in the Regulation of the Council of Ministers of 31 October 2018 on Serious Incidents Thresholds (Journal of Laws of 2018, item 2180).

Pursuant to Article 13 of the NCSA, an operator of an essential service may provide the relevant CSIRT MON, CSIRT NASK or CSIRT GOV with information concerning: 1) other incidents; 2) cybersecurity threats; 3) risk estimation; 4) vulnerabilities; 5) the technologies used. The said information shall be transmitted electronically and if impossible - with the use of other available means of communication. Where a sectoral cybersecurity team is appointed, an operator of an essential service may simultaneously transmit any such information to the team, in electronic form. An operator of an essential service shall also classify the information that constitutes legally protected secrets, including information constituting trade secrets.

A trade secret shall be construed as the technical, technological and organisational information of a company or other information of economic value, which as a whole or in a specific configuration and collection of its elements is not generally known to persons regularly dealing with that type of information, or is not easily accessible to such persons, provided that the person authorised to use or dispose of such information has undertaken, with due diligence, actions to maintain its confidentiality – Article 11(2) of the Act of 16 April 1993 on Combating Unfair Competition (i.e. Journal of Laws of 2020, item 1913, as amended).

Legally protected secrets also include classified information. Classified information is information the unauthorised disclosure of which would or could cause damage to the Republic of Poland or would be detrimental from the point of view of its interests, also in the course of its preparation and regardless of the form and manner of its expression, which follows from Article 1 of the Act of 5 August 2010 on the Protection of Classified Information (consolidated text: Journal of Laws of 2019, item 742 as amended.), hereinafter referred to as the APCI. According to the judgement of the Supreme Administrative Court dated 8 March 2017, I OSK 1777/15 (LEX no. 2338895), in order to recognise a piece of information as classified, it is enough that a substantial component is involved, therefore, the existence of such quality by which it will constitute information, the unauthorised disclosure of which, would or could cause damage to the Republic of Poland or would be detrimental in the context of its interests, also in the course of its preparation and regardless of the form and manner of its expression. The substantial component – which stems from the position expressed by the Regional Administrative Court in the judgement of 8 January 2020, II SA/Wa 1385/19 (LEX no. 3078853) – makes it possible to recognise a given piece of information as classified. Classified information shall therefore be protected regardless of whether the authorised person found it appropriate to give it an adequate level of confidentiality. It shall be classified because of the threats resulting from its content or from the manner in which it was obtained, and not as a result of its classification and level of confidentiality.

Pursuant to Article 4 of the APCI, classified information can be made available only to a person who provides a guarantee of confidentiality and only to the extent necessary for that person to perform work or duty on the position held, or to perform the commissioned activities. The legislators restrict access to classified information as regards the subject to persons who provide a guarantee of confidentiality, thus those who meet the requirements imposed by the Act for the purpose of protection of classified information against unauthorised disclosure, confirmed as a result of the conducted verification procedure, and also as regards the object – to classified information required for such persons to perform their work or service on the position held, or to perform the commissioned activities. Pursuant to Article 4 of the APCI, a person who, as a result of the verification procedure conducted towards it, has obtained a security clearance authorising access to classified information with a specific level of confidentiality, is not authorised to access all classified information with such a level (or a lower one), but only the information necessary for the performance of official tasks (Stankowska, 2014: LEX/el.).

4 Conclusion

The objective of the National Cybersecurity System, as defined in Article 3 of the NCSA, is to ensure cybersecurity at the national level, including the uninterrupted provision of essential services and digital services by achieving the appropriate level of security of the information systems used to provide these services, and by ensuring the successful handling of incidents. This provision sets the general objective of the National Cybersecurity System as ensuring cybersecurity at the national level. It also points to

examples of specific objectives: (1) uninterrupted provision of essential services; (2) uninterrupted provision of digital services (Szpor, 2019b: LEX/el.).

Pursuant to Article 2(4) of the NCSA, cybersecurity is the ability of information systems to resist any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems. Cybersecurity is a term pertaining to providing protection and preventing the threats that affect cyberspace itself, as well as functioning in cyberspace, which applies to both the public and private sectors and their interactions (K. Chałubińska-Jentkiewicz, 2019: 21). Cyberspace is not only becoming a place where people work, gain knowledge, communicate with each other and seek entertainment, but it has also become a place where people are exposed to various threats (Pieczywok, 2019: 227). State security in cyberspace must be a primary determinant of the activities of relevant services responsible for the protection of strategic information systems.

Cybersecurity as an element of the state security in the era of the information society and widespread computerisation of public entities should be treated as a strategic element taken into account when building the National Security System, as the scale of cyber threats and their effects may significantly affect the normal functioning of the state.

References:

Bożek, M., Karpiuk, M., Kostrubiec, J. & Walczuk, K. (2012) *Zasady ustroju politycznego państwa* (Poznań: Polskie Wydawnictwo Prawnicze IURIS).

Chałubińska-Jentkiewicz, K. (2019) *Cyberodpowiedzialność* (Toruń: Wydawnictwo Adam Marszałek).

Chałubińska-Jentkiewicz, K., Karpiuk, M. & Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* (Maribor: Institute for Local Self-Government), https://doi.org/10.4335/2021.5.

Czuryk, M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity, *Cybersecurity and Law*, 2, pp. 39-50.

Karpiuk, M. (2020) The obligations of public entities within the national cybersecurity system, *Cybersecurity and Law*, 2, pp. 57-72.

Karpiuk, M. (2021b) The Organisation of the National System of Cybersecurity: Selected Issues, *Studia Iuridica Lublinensia*, 30(2), pp. 233-244, http://dx.doi.org/10.17951/sil.2021.30.2.233-244.

Kostrubiec, J. (2021) The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-government in Poland, *Lex Localis – Journal of Local Self-government*, 19(1), pp. 111-129, https://doi.org/10.4335/19.1.111-129(2021).

Pieczywok, A. (2019) Cyber threats and challenges targeting man versus his education, *Cybersecurity and Law*, 1, pp. 225-236.

Szpor, G. (2019a) Komentarz do art. 4, In: Czaplicki, K., Gryszczyńska, A. & Szpor G. (eds.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: Wolters Kluwer), LEX/el, available at: https://sip.lex.pl/#/commentary/587786646/584086 (May 21, 2022).

Szpor, G. (2019b) Komentarz do art. 3, In: Czaplicki, K., Gryszczyńska, A. & Szpor G. (eds.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: Wolters Kluwer), LEX/el, available at: https://sip.lex.pl/#/commentary/587786645/584085 (May 21, 2022).

Stankowska, I. (2014) *Ustawa o ochronie informacji niejawnych. Komentarz* (Warszawa: Lexis Nexis).