LEX LOCALIS

The Public Dimension of Cybersecurity

Editors:
Mirosław Karpiuk
Jarosław Kostrubiec


§
LEX
LOCALIS

Title: The Public Dimension of Cybersecurity

Editors: prof. dr. habil., Mirosław Karpiuk, Ph.D. (University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration), assoc. prof. dr. habil., Jaroslaw Kostrubiec, Ph.D. (Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration)

Reviewers: assoc. prof. dr. András Bencsik, Ph.D. (Eötvös Loránd University (Budapest), Faculty of Law, Hungary), assoc. prof. dr. Pawel Sitek, Ph.D. (University of Economics and Human Sciences in Warsaw, Poland)

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID 117820931
ISBN 978-961-7124-10-1 (PDF)

First published in 2022 by
Institute for Local Self-Government Maribor
Smetanova ulica 30, 2000 Maribor, Slovenia
www.lex-localis.press, info@lex-localis.press

For Publisher:
assoc. prof. dr. Boštjan Brezovnik, director

Price: free copy

Acknowledgement:
The monograph has been prepared as a result of the research project "The place of cybersecurity in the public realm. The European dimension" supported by the Institute for Local Self-Government Maribor, Slovenia.

https://doi.org/10.4335/2022.1 ISBN 978-961-7124-10-1 (PDF)

Available online at http://www.lex-localis.press.

The Public Dimension of Cybersecurity

Editors:
Mirosław Karpiuk
Jarosław Kostrubiec

Maribor, 2022

The Public Dimension of Cybersecurity

MIROSŁAW KARPIUK & JAROSŁAW KOSTRUBIEC

Abstract The development of new communication technologies also entails new threats in the form of various cyber crises caused primarily by external factors that affect both public entities (including states and public administration authorities) and private entities. These crises are also political and military in nature, threatening state sovereignty. Therefore, states must strive to ensure cybersecurity, which cannot be limited to the administrative boundaries of individual states alone, as cyberthreats are transnational in nature. Cybersecurity, understood as the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems, must be a priority for action in the public sphere to adequately secure the cyberspace against attacks. It must also be a fundamental component in public policy implemented at all levels of governance, be they central, regional or local.

Keywords: • cybersecurity • cyberspace • digital competence • information protection

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl. Jarosław Kostrubiec, Ph.D., Dr. Habil. University Professor, Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration, Plac Marii Curie-Skłodowskiej 5, 20-031 Lublin, Poland, ORCID: 0000-0003-1379-9846, e-mail: jaroslaw.kostrubiec@mail.umcs.pl.

https://doi.org/10.4335/2022.1 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

Table of Content

Introduction

Nowadays, cyberspace has become a sphere that significantly influences public, private, social and professional life. Not only does it allow people from different parts of the world to communicate quickly, but it also facilitates, and sometimes even enables, business activities. In connection with its crucial role, it is important to ensure the security of all entities using it. To safeguard the normal functioning of both the state and society, cybersecurity must be adequately protected. Here, it must be recognised that cybersecurity includes not only activities necessary to protect information systems from cyberthreats, because the scope of such protection also covers the users of these systems, as well as other entities.

The National Security Strategy of the Republic of Poland clearly indicates the need to increase the level of resilience to cyberthreats and to enhance the level of information protection in the public, military and private sectors, as well as the need to promote knowledge and good practices enabling citizens to better protect their information (including information concerning them).

Cyberattacks on public sector information systems may undermine the stability of the state and its institutions, and therefore the state must not only constantly monitor cyberthreats, but also have appropriate protection measures in place to respond to the danger. The state must, among other things, secure the fulfilment of tasks for defence, security and public order, and will therefore aim to protect networks and systems of strategic importance.

The strategic objectives, as well as the relevant policy and regulatory measures that need to be implemented to ensure the resilience to cyberthreats of information systems, operators of essential services, critical infrastructure operators, digital service providers as well as public administration are set out in the Cybersecurity Strategy of the Republic of Poland. Its main objective (similarly to the National Security Strategy of the Republic of Poland) is to increase the level of resilience to cyberthreats and the level of information protection, including that in public space. Under the specific objectives, it identifies, among others: developing a national cybersecurity system; raising the level of resilience of public administration information systems and achieving the ability to effectively prevent and respond to incidents; increasing the national potential in the field of cybersecurity technologies; building public awareness and competence in the field of cybersecurity; achieving a strong international position of the Republic of Poland in the area of cybersecurity. Therefore, the objectives that the state should pursue in the field of cyberspace security include, first and foremost, strengthening the ability to counter cyberthreats (including those in the public sphere), which is linked to the creation of strategic national networks and systems to limit cyberattacks.

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 (Bake, 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).

LEX LOCALIS

The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity

DOMINIK TYRAWA

Abstract Cybersecurity is one of the types of security that is distinguished in the field of legal sciences with respect to the legal aspects of security. This type of security is very extensive and specialised in nature. Apart from the specialised and precise legal language employed, by using approaches derived from the field of communication and information sciences, the sphere of values that underlie this type of security can also be distinguished. The variety of goods that are protected under cybersecurity leads to the multi-faceted nature of the applicable solutions in this regard. This multi-faceted character refers both to the material scope, namely, the goods that are protected in this way with the application of optimised tools, and to the subjective scope, namely, the entities protected by the system and by which entities it is protected. All these analyses clearly indicate that this involves a very complex phenomenon which is highly relevant to our daily lives.

Keywords: • axiology • security • cybersecurity • systemic • material and procedural aspects of cybersecurity • man vs state

CORRESPONDENCE ADDRESS: Dominik Tyrawa, Ph.D., Dr. Habil., University Professor, John Paul II Catholic University of Lublin, Faculty of Law, Canon Law and Administration, Department of Administrative Law, al. Racławickie 14, 20-950 Lublin, Poland, e-mail: dominik.tyrawa@kul.pl, ORCID: 0000-0001-6385-9726.

https://doi.org/10.4335/2022.1.2 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Security is one of the most important human needs. The literature on the subject, both in legal sciences, and in other disciplines (psychology, economics, management, sociology, security sciences), when describing the need for security, usually refers to A. Maslow's hierarchy of needs. This is based on the fulfilment of physiological needs, examples of which include the need for food, housing, clothing and procreation. The nature of these needs ensures that they have the strongest impact on man, and man first strives to satisfy them. It is only after fulfilling the primary needs that the will to satisfy other needs appears in man. Maslow, in creating a hierarchy of these, identified first the need for safety, then the need for belonging and love, the need for esteem and finally the need for self-actualisation. The need for safety is expressed in the search for safety and constancy, and then comes down to the pursuit of dependence, the search for protectiveness, the avoidance of unclear situations, the avoidance of chaos, the pursuit of law and order and the rule of law (Maslow, 2009: 65-71).

It should be noted that nowadays, even before the outbreak of the global COVID-19 pandemic, the need for security was often overlooked or taken for granted. In developed societies, human life was rather stable and physiological needs were more or less, met. For many people, social emphasis was on the "self" and psychological needs, and security itself was marginalised Only a threatening situation concerning law, order or authority could trigger a return to the need for security and treating it not as something obvious, but as something desirable (Tyrawa, 2018: 37).

The outbreak of the COVID-19 pandemic prompted a return to the source, and increased research into the multifaceted nature of the need for security, including that in the legal sciences, met with greater scientific interest. Somewhere in the background of this research, on its margins, there are activities and research in the field of cybersecurity. This concept naturally interacts with research related to the pandemic (for example, through the increased importance of communication and information systems and networks, in the context of e-learning, home-office, general security of business transactions, work provision, fulfilment of various types of obligations (mainly civil law obligations), when supply chains are interrupted or hindered), although it should be emphasised that research in this field was successfully conducted even before the outbreak of the pandemic.

The purpose of this paper is to indicate what cybersecurity is, how it should be embedded in the legal security system, what key values underlie the concept and how, through strictly defined institutions, the concept should be protected and guaranteed.

2 The concept of cybersecurity and its place in the legal security system

In the search for a definition of cybersecurity, the normative solutions of a given country (in this case the Republic of Poland) should be analysed first, followed by the views of legal commentators and possibly case law. It should be noted, however, that defining cybersecurity is not the main task of this paper and therefore the definitions referred to will be of a general nature and certainly not exhaustive.

The basic act on cybersecurity, in force since July 2018, is the National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended). This normative act primarily organises issues related to cybersecurity at the national level. First of all, the Act introduces an extensive set of specialised concepts and specifies more precisely the system of entities covered by this systemic protection. Furthermore, the legislator points out the problem of identification and registration of operators of essential services, the duties of operators of essential services, digital service providers and public entities, and specifies the tasks of specialist entities more precisely, i.e. CSIRT MON (Computer Security Incident Response Team operating on a national level, managed by the Minister of National Defence), CSIRT NASK (Computer Security Incident Response Team operating on a national level, managed by the Research and Academic Computer Network – National Research Institute) and CSIRT GOV (Computer Security Incident Response Team operating on a national level, managed by the Head of the Internal Security Agency). In addition, it clarifies the principles of sharing information and processing personal data, and introduces and systematises the system of competent authorities for cybersecurity, the tasks of the minister in charge of computerisation, the tasks of the Minister of National Defence, as well as the issues of supervision and control of operators of essential services, digital service providers and entities providing cybersecurity services. The last relevant regulations of the aforementioned Act refer to the establishment of competent authorities for cybersecurity, i.e. the Plenipotentiary, whose task is to coordinate activities and implement the government's policy on cybersecurity; and the Committee, i.e. the opinion and advisory body in the field of cybersecurity, acting at the Council of Ministers. Beyond the aforementioned, it lays out the Strategy, i.e. the document that defines strategic objectives and relevant policy and regulatory measures aimed at achieving and maintaining a high level of cybersecurity. The final section of the Act relates to the provisions on fines.

The very description of the material scope above indicates that the stated Act is fundamental in the field of cybersecurity. At the same time, it should be noted that the regulation of such a broad material and subjective spectrum raises the question of whether this is a regulation that provides an exhaustive coverage of the issues contained in the title or a regulation that attempts to order these issues. Answering this question goes beyond the scope of this paper, although according to the Author, a statement about ordering these issues would be more appropriate.

In the context of this paper, the most important element is to specify more precisely what cybersecurity is. In the aforementioned Act, in Article 2(4), cybersecurity is defined as the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. This case involves a de facto normative mental construct denoting the security of IT systems and networks (Banasiński, 2020: 16).

Legal commentaries approach this concept in a slightly different way. The basic policy paper of the Republic of Poland in this regard defines this concept as "a process of ensuring the secure functioning in cyberspace of the state as a whole, its structures, natural persons and legal persons, including entrepreneurs and other entities without legal personality, as well as the communication and information systems and information resources at their disposal in global cyberspace" (National Security Bureau, 2015: 7-8). At the same time, the paper identifies the main objective in terms of cybersecurity as ensuring the secure functioning of the Republic of Poland in cyberspace, including an adequate level of security of national communication and information systems, especially the ICT critical infrastructure of the state, as well as private economic entities that are key to the functioning of society, in particular, those that are part of the financial, energy and health care sectors (National Security Bureau, 2015: 9).

It seems that a proper definition of cybersecurity should be linked to the concept of security in the first place. When defining the concept of "security", it should be pointed out that it refers to a number of semantic levels (Potrzeszcz, 2013: 25), and is also related to the fact that this case involves a common phenomenon in the everyday lives of individuals and societies, so the concept will be defined more precisely by intuition and will be difficult to define unambiguously (Potrzeszcz, 2014: 15). In addition, it should be noted that security is defined in various ways within the methodology of various sciences, making the concept of security all the more ambiguous. Due to the limited nature of this paper, it may be assumed that security is a state of peace, a state that gives a feeling of certainty, and a state that guarantees its maintenance. Security is the opposite of chaos or uncertainty.

Cybersecurity, then, is a state of constancy, security and peace in cyberspace. Cyberspace should be understood as a communication space that is created by online connection systems and allows people to communicate online and establish relationships in real time. Cyberspace is also an environment in which information is exchanged through networks and computer systems. This is a dimension of activities in which all actions diverge from the physical environment. This is a new dimension (in addition to the terrestrial, aquatic, air, and space environments) in which various actions, including military actions, can be carried out. This environment differs from those mentioned above primarily in that: 1) it is man-made; 2) its participants have full control over the nature of this environment; 3) it has no territorial limitations. In addition, cyberspace has four typical features: 1)

anonymity; 2) aterritoriality; 3) regularity; 4) global reach (Marczyk, 2018: 59-60). The concept of cybersecurity, which benefits most from the conceptual framework of the law of new technologies, situated within administrative law, consists of institutions of constitutional, substantive and procedural law.

In situating cybersecurity within the national security system, it should first be pointed out that cybersecurity is a specialised branch of security that includes the protection of information systems from threats (Czuryk, 2019: 42). It seems that the assumption that cybersecurity is one of the types of security is most correct. The most commonly identified types of security include: international security, state security, public security, legal security, environmental security, energy security, economic (and social) security, political (and military) security, personal security, aviation security, local security, cultural security, ICT security and health security (Tyrawa, 2018: 80-109). However, it should be stressed that these concepts are intertwined. It is impossible to set precise and fixed boundaries in this respect. In addition, the terminology is imprecise (various ways of defining a given type of security, in this case, ICT security and technological security are conceptually similar), which makes it even more difficult to analyse individual types of security.

The above reasons clearly indicate that in relation to cybersecurity, it is one of the types of security that is intertwined to varying degrees with other types of security, to the greatest extent with international security, state security, public security, energy security and aviation security. In this case, we are faced with a very specialised concept that primarily refers to an artificial man-made system based on ICT solutions.

3 The multi-faceted nature of cybersecurity

When describing the material scope (the tasks to be fulfilled by a given type of security) and the subjective scope (both the entities in relation to which a given type of security applies and the entities that carry out activities in this respect) of cybersecurity, it should first be noted how multi-faceted this phenomenon is. The material scope and subjective scope are intertwined. The material scope will be presented in detail in the next part of this paper, as will be with regard to the subjective scope. The considerations in this respect, however, must be preceded by general remarks.

When answering the question of what cybersecurity is and what the multi-faceted nature in this regard is, the analysis should begin with the material scope. The gradation of the goods that this type of cybersecurity protects can essentially be reduced to the protection of human life and health. This is expanded into individual protected goods. Their differentiation is basically an analysis of individual phenomena, where communication and information systems and networks are used. Due to the limited and introductory nature of the paper, an attempt to specify all the specific goods protected in this way is

doomed to fail. Nevertheless, it can be stated that at the end of every cybersecurity activity there is a human being.

A specific example is the situation involving the ICT protection of a given information system, i.e. a communication and information system, referred to in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks (consolidated text, Polish Journal of Laws of 2020, item 346, as amended). First of all, an extensive security system is put in place to protect a specific system (and thus the information contained in it, partly related to a specific human being). Further protection concerns the possibility of using the system, at the level of performing tasks by public administration, as well as in relation to an individual being whose sensitive data is included in the system. In addition, it should be pointed out that detailed data, first of all personal data, is protected. To sum up, this case involves multilevel protection of various goods, and in particular, protection of the organisational structure itself, which operates on the basis of these systems, and ultimately this protection concerns an individual who, being part of a given organisational structure, performs tasks on the basis of this system, as well as an individual whose sensitive data is included in this system.

In terms of the subjective scope, the multi-faceted nature of cybersecurity should be understood as an extensive system of subjective protection in this respect. It seems that it can be assumed that, first of all, cybersecurity protects communication and information systems and the individual who uses them, as well as the individual's data collected in the course of operating these communication and information systems. Another definition of a communication and information system can be mentioned here, according to which it is a set of cooperating IT devices and software that enables processing and storage, as well as sending and receiving of data via telecommunications networks by using terminal equipment that is appropriate for a particular type of network, and this definition is based on Article 2(3) of the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344, as amended). Terminal equipment, in accordance with Article 2(43) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Polish Journal of Laws of 2021, item 576, as amended), should be understood as telecommunications equipment intended to be connected directly or indirectly to network terminations.

Subjective protection in this respect can be described as individual (private), mixed (private-public) and collective (public, state or supranational) protection. Individual protection is organised by such an entity, i.e. a person, e.g. by purchasing and installing antivirus software on the computer they use, or by another private entity, e.g. a company, organising its own internal communication and information system and securing it in an appropriate manner. Mixed protection is protection involving the cooperation of private entities (e.g. ICT companies, both local and global) with entities operating within the state structure (e.g. local government units or public administration authorities). Private entities as part of this cooperation provide specific know-how, and state entities are most

often the entities that order a widely understood service. Cooperation in this respect may take place within a small organisational unit and a telecommunications or IT company, but also at the state level (cooperation between the state and a global ICT company) or even supranational, where the customer is an international organisation, such as the European Union. The last type of protection is collective protection, which is guaranteed in its entirety by a local government unit, public administration or an international organisation. Determining the precise boundaries between these types of protection is in some cases difficult, as within this issue, various factual phenomena intermingle that are difficult to fit into a specific security model.

4 Values protected by cybersecurity

As already stated above, the fundamental and main good to be protected by cybersecurity is man, and, more specifically, their life and health. The presented case involves goods that can be placed highest in the hierarchy of values important for man. Without protection of human life or health, other goods recede to the background, and their protection becomes pointless.

In terms of subject matter, cybersecurity consists primarily of instruments, specialised computer programs and systems that collect relevant data. Their presentation and precise specification at this point goes beyond the scope of the paper. However, a general framework for this issue can be outlined. When indicating the instruments that are employed, they can generally be defined as the use of the Internet and other networks (Intranet, Extranet), as well as computers, phones, smartphones, tablets, servers, terminals or smart TV. These instruments are applied in order to better satisfy human needs, improve the quality of life, maximise profit (both on the part of public administration and on the part of citizens) and, above all, guarantee an increase in the efficiency and effectiveness of administration. These instruments are employed in the development of, for example, e-business, e-administration, e-health, e-culture or e-tourism.

Public administration, acting in the field of cybersecurity, uses systems involving the application of satellite telecommunications, including, for example, location, environmental monitoring and security, in the field of road, sea, air transport, in relation to the transport of dangerous goods, livestock, in the field of civil defence, crisis management, humanitarian aid, in relation to agriculture, land measurement, land surveying and land register. Other areas where communication and information systems are implemented include the extraction and distribution of fossil fuels (oil and gas), search and rescue, as well as such areas as logistics, environment, science or law enforcement.

The state is involved in the development of information society (and thus also in the development of cybersecurity), through the development of information technologies, within administration itself, in the area of its contacts with citizens, as well as in the state's investment in telecommunications infrastructure. Actions in this regard are aimed at

solving related problems. In this respect, first of all, the following aspects should be mentioned: eliminating digital exclusion, protecting consumers in electronic commerce, combating computer crime, developing electronic payment systems, respecting individual privacy and protecting intellectual property rights.

The scope concerned also includes extremely important communication and information systems that are used by public administration or individuals on a daily basis, i.e. KRS (National Court Register), KRK (National Criminal Register), NKW (New Land and Mortgage Register), PESEL (Universal Electronic System for Registration of the Population), POLTAX (a distributed system for recording and processing data on taxpayers used by tax offices), CEPiK (Central Register of Vehicles and Drivers) or REGON (Register of National Economy – National Official Register of Business Entities).

It is correct to say that the main task of administrative law is to serve man (Zimmermann, 2013: 77). This extremely general statement can also be related to the tasks that form the axiological basis of security. Referring to cybersecurity, it can be stated that the systems used by public administration protect, in the first place, data relating to the status of an individual in terms of their health status, property status (information on real property held, its location, vehicles, their mileage), data on marital status and family members, data on the address of residence (permanent address or actual residence), data on financial and economic status, data on social benefits received or data on documents used by the individual (passport, identity card, driving licence, vehicle registration certificate). Cybersecurity thus protects the part of an individual's life that can be described as "privacy".

5 Entities protecting cybersecurity – general considerations

An element complementing the considerations in the field of cybersecurity is the indication (emphasis on) of the entities that act for cybersecurity. As already stated, three types of protection can be distinguished in this regard, i.e. individual, mixed and collective protection.

Individual protection relates both to natural persons and legal persons, but also to entities without legal personality. As a rule, state action in this respect is very limited. It is the individual course of action that can be described as private (also in terms of the financial resources involved) that is key in this regard. The role of the state in this aspect should be limited to two problem areas, educational – where the state highlights and educates about cyberthreats, and training – where the state trains individuals, who then educate the public about such threats.

The second type of protection is mixed private-public protection. Its importance in the globalised world is constantly growing. This is a matter of the space that needs to be

described in detail in order to diagnose the threats and opportunities associated with its development. It is in this space that we can look for entities that will be described as hybrids of public-private transnational bodies. It seems that within this area of cooperation, it is possible to identify in more detail such entities as: formal intergovernmental regulatory bodies, informal intergovernmental regulatory networks for cooperation and coordination of arrangements, national regulatory bodies operating with reference to international intergovernmental regimes, hybrid public-private regulatory bodies, and some private regulatory bodies exercising transnational governance functions of particular public significance. The fact of distinguishing these entities is based on the contemporary needs of the international community, because transgovernmental administration is also in place, due to global interdependence (Kingsbury, Krisch, Stewart, 2005: 16).

The third type of subjective protection is collective protection. Protection in this respect is guaranteed by an entity being part of a national, supranational or international structure. In the case of supranational or international structures, such entities as the EU, NATO or the UN can be mentioned, for example. State protection is much more extensive. Entities that can be classified in this group include local government units and entities dependent on them (e.g. budget enterprises, municipal companies, but also schools or kindergartens, cultural institutions or others), central or local public administration, courts, prosecutor's offices, court enforcement officers supervised by courts with territorial jurisdiction. The secret services play very important roles in this respect. The gradation of public administration activities in the field of cybersecurity can be linked to the gradation, not only of the entities established for this purpose, but, above all, to the development (gradation) of the manner of operation of a particular entity. In this regard, traditional government (which includes the administration itself), which is based on paper documents, and higher organisational forms can be identified. The latter include e-government (including e-administration), based on static ICT tools and Internet 1.0, Government 2.0, based on Internet 2.0 and social media, and M-government (mobile government), which is built on mobile information technologies (Khan, 2015: 135-149).

A large number of entities performing cybersecurity tasks are specified in Article 4 of the Act on the National Cybersecurity System. Such agencies are components of a system identical to the specification that was made in the text in terms of classification as actors involved in state protection. As already brought forward, subjective protection is multifaceted in nature. The values protected by these entities are part of the system of values that underlie cybersecurity as a type of security.

6 Conclusion

As stated in the text, the phenomenon of the multi-faceted nature of cybersecurity can be readily identified. This nature is both material and subjective. The values that cybersecurity should protect are crucial in this case. The most important good protected

in this way is the protection of individual privacy, but also the protection of health and life. Both private and public entities should tailor protective measures to the good to be protected and the threats that may affect it. Building a proper system in this respect, based on the tools available, is a challenge in times of growing threats to electronic security, especially in terms of the extensive digitalisation of social life.

References:

Banasiński, C. (2020) Prawne i pozaprawne źródła wymagań dla systemów cyberbezpieczeństwa, In: Banasiński, C. & Rojszczak, M. (eds.) *Cyberbezpieczeństwo* (Warszawa: LEX a Wolters Kluwer business), pp. 15-38.

Biuro Bezpieczeństwa Narodowego (2015) *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej* (Warszawa: Centrum Poligrafii Sp. z o.o.).

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.

Khan, G.F (2015) The Government 2.0 utilization model and implementation scenarios, *Information Development*, 2, pp. 135-149.

Kingsbury, B., Krisch, N. & Stewart, R.B. (2005) The Emergence of Global Administrative Law, *Law and Contemporary Problems*, 68, pp. 15-61.

Marczyk, M. (2018) Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, *Przegląd Teleinformatyczny*, 1-2, pp. 59-72.

Maslow, A. (2009) *Motywacja i osobowość* (Warszawa: Wydawnictwo naukowe PWN).

Potrzeszcz, J. (2013) *Bezpieczeństwo prawne z perspektywy filozofii prawa* (Lublin: Wydawnictwo KUL).

Potrzeszcz, J. (2014) *Bezpieczeństwo i porządek publiczny w ujęciu filozofii prawa*, In: Lis, W. (ed.) *Bezpieczeństwo państwa. Zagadnienia podstawowe* (Lublin: Wydawnictwo KUL), pp. 15-34.

Tyrawa, D. (2018) *Gwarancje bezpieczeństwa osobistego w polskim administracyjnym prawie drogowym* (Lublin: Wydawnictwo KUL).

Zimmermann, J. (2013) *Aksjomaty prawa administracyjnego* (Warszawa: LEX a Wolters Kluwer business).

LEX LOCALIS

Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats

KRZYSZTOF KACZMAREK

Abstract False, fast-spreading information can mould public sentiment, influence the outcomes of democratic elections, cause tensions in the international arena, and even spark armed conflicts. The degree to which a state is vulnerable to such threats depends largely on the digital competence of that state's general public. Digital competency includes information competencies, which involve the ability to obtain, evaluate and apply information. Deficits in the public's information competencies make the state more vulnerable to be targeted by disinformation – an element of hybrid warfare. This is especially important because there are no technical measures which could be used to counter disinformation online. It seems that the only way to make the state more resilient against cybersecurity threats is by improving the digital competencies, including, in particular, information competencies, of the general public. This, however, requires strong educational outcomes across all educational stages.

Keywords: • digital competencies • information competencies • manipulation • disinformation • cybersecurity • hybrid warfare

CORRESPONDENCE ADDRESS: Krzysztof Kaczmarek, Ph.D., Koszalin University of Technology, Faculty of Humanities, Department of Regional and European Studies, Śniadeckich 2, 75-900 Koszalin, Poland, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

https://doi.org/10.4335/2022.1.3 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Information manipulation is not a new phenomenon. From time immemorial, people have tried to influence and mislead others to achieve their specific ends. The influence patterns used in the past – tied so strongly to human nature and taking advantage of the perceptual weaknesses of humans – continue to be deployed successfully to influence societies and international relations, among others. Initiated by individuals, pressure groups, and entities, deception and misleading are popular means by which to elicit a desirable reaction from the general public. The emergence of new technologies facilitating information flow has greatly expanded the possibilities of influencing members of the public – for instance, through provocations, spreading false information and falsifying data. An enormous leap has been made away from traditional media – press, radio, and television – and towards the Internet, making it possible to send any information, true or false, into the world in a matter of seconds. Cyberspace has become the primary channel for information flow, allowing almost anonymous interferences with information flows (e.g. distorting messages or discrediting certain groups). The Internet can also be used to generate essentially false information, addressed to any target group – locally, regionally and globally – to produce specific effects that are intentional and often harmful to the general public. Moreover, we should not forget about the ever-growing risk of cyberattacks, which are increasingly having impact on public safety. Also of concern is the employment of advanced computer programs to modify source materials (deepfakes), making it easy to discredit public figures, such as politicians and celebrities, or even neighbours.

The more the public is aware about the potential threats, and the more knowledge it has of the cyberspace, the less prone it is to being manipulated. Clearly, one important measure to tackle cyberthreats (such as deepfakes) is to provide younger generations with proper education by devising curricula that teach them to search for and double-check information, as well as to instil the principles of communication. This is where digital competencies of the general public come to the fore – their improvement now seems to be the key objective of security, educational and social policies.

2 Digital competencies vs. information competencies

Technological advancements in access to information have made digital competencies one of the key determinants of the quality of life. Social activity now largely relies on the Internet. Digital artefacts and access to the Internet influence almost all aspects of social and private lives. Yet, cyberspace is not the natural environment of humanity. Consequently, no tradition exists of passing knowledge about the phenomena and processes occurring in cyberspace to future generations. However, in order to analyse how the digital competencies of the general public influence the state's vulnerability to cyberthreats, these competencies need to be defined. It can be assumed that digital competencies include: 1) browsing, searching for, and filtering digital data, information

and content; 2) evaluating digital data, information and content; 3) managing digital data, information and content; 4) interacting through digital technologies; 5) sharing through digital technologies; 6) civic engagement through digital technologies; 7) cooperating through digital technologies; 8) netiquette; 9) digital identity management; 10) creating digital content; 11) copyrights and licensing; 12) computer programming; 13) security technologies; 14) personal data and privacy protection; and 15) the ability to solve technical problems.

According to information provided on the Chancellery of the Prime Minister's website (KPRM), digital competencies include: 1) IT competencies – the ability to use devices and software; 2) information competencies – the ability to use online information critically; and 3) functional competencies – the ability to apply the aforementioned competencies in everyday private and professional life (KPRM, 2020).

Contemporary digital devices and the systems that manage them do not require the average user to have extensive knowledge of IT systems and advanced technical skills. Nevertheless, as modern technology continues to evolve, there is a continuing need to stay up-to-date. This particularly concerns the ability to double-check information, especially since fast-spreading false information can cause social unrest and spark armed conflicts. Researchers concerned with this area have stressed that the growing scale of disinformation poses one of the greatest challenges for global security (Aronhime, Cocron, 2021). Also, it is worth emphasising that technology is not the only factor involved in the susceptibility of the general public (or certain sections thereof) to disinformation. Other factors come into play as well, and they are psychological, cultural, economic and political in nature (Tomala, 2021).

A low level of information competency can make the public more susceptible to fake news, whose primary aim is to undermine the authority of the state and trust in its institutions, as well as to shape public opinion by perpetuating a state of apprehension. Fighting disinformation represents a challenge for both public institutions and private businesses. It seems, however, that institutionally implemented legal solutions cannot counter this phenomenon. What is fundamentally important is that there is common awareness among the public that each piece of information found online should be approached critically. This is particularly pertinent to emotionally charged information, such as that involving religion, ethnicity - and vaccination against COVID-19.

According to some researchers, in the context of cybersecurity, the threats posed by information manipulation seem to be more serious than those associated with malware. Indeed, no technical measures exist to protect against such manipulation (Kangasniemi, 2020).

3 Digital competencies of European societies

Digital competencies are becoming increasingly important in today's world. However, there has been little progress in the European Union in recent years as far as improving the basic digital competencies of adult Europeans is concerned. Even though the European Commission has supported Member States and provided them with guidance, there are relatively few EU-funded projects focusing on the basic social skills of adults.

In 2019, a total of more than 75 million working-age adults in Europe did not have at least basic digital skills. This mostly included the elderly, the undereducated and the unemployed. Meanwhile, more than 90% of jobs already require at least basic digital skills.

The European Commission has implemented a number of measures since 2015 to improve the digital skills of European citizens. Between 2016 and 2018, national projects as part of the "Digital Skills and Jobs Coalition" provided almost 11 million Europeans with the opportunity to improve their digital skills. Almost half of them were primary and secondary school students. However, no data exists as to how these measures ultimately influenced the objectives of this initiative.

Efforts in specific areas of basic digital skills for adults are often part of broader initiatives. This makes it impossible to determine the total amount of EU funds spent exclusively for this purpose. Nevertheless, existing data suggest that the resources available specifically for efforts to improve digital skills among adults are relatively scarce – for instance, projects that specifically involved teaching digital skills in Member States represented only about 2% of the European Social Fund's overall budget for 2014-2020, even though they enjoy a priority status.

Table 1: The percentage of European residents with at least basic digital skills in 2019

Country	Percentage of individuals who have basic or above basic overall digital skills
European Union – 27 countries (from 2020)	56
Belgium	61
Bulgaria	29
Czechia	62
Denmark	70

Germany	70
Estonia	62
Ireland	53
Greece	51
Spain	57
France	57
Croatia	53
Italy	42
Cyprus	45
Latvia	43
Lithuania	56
Luxembourg	65
Hungary	49
Malta	56
Netherlands	79
Austria	66
Poland	44
Portugal	52
Romania	31
Slovenia	55
Slovakia	54
Finland	76
Sweden	72
Iceland	85
Norway	83
Switzerland	77
United Kingdom	74

North Macedonia	32
Albania	21
Serbia	46
Turkey	36
Bosnia and Herzegovina	24
Kosovo	28

Source: (Eurostat, 2021).

In all these countries, the biggest deficits in digital skills were associated with searching for and verifying information online, as well as familiarity with the basic safety rules and measures (Techrush, 2021). The deficits varied, however, between states.

Despite the Member State's investments made in recent years to develop digital infrastructure for educational and training purposes, significant differences continue to exist both between and within the Member States. Contrary to popular belief that young people are the digital generation, study results have shown that a large part of this population have underdeveloped digital skills. Indeed, in all the studied countries, more than 15% of all students did not have adequate digital skills (European Commission, 2020). Moreover, according to OECD data, secondary school teachers in Europe rarely receive training in the use of ICT for educational purposes, and teachers themselves have voiced their need to develop professionally in terms of ICT skills (Europa Nu, 2021). These data suggest that there is no significant correlation between the age group and digital competence. Each group includes people with different levels of knowledge and skills.

4 Threats associated with deficient digital competencies of the general public, with special focus on information competencies

Cyberspace threats to the functioning of societies and states stem not from the existence of ICT infrastructure *per se*, but from the possibilities it affords. In the literature on this subject, the seven most-mentioned sources of cyberattacks include: 1) states – cybernetic attacks launched by a state against another state can disrupt communications, operations of state services and everyday lives of citizens. Here, an attack may be part of hybrid warfare; 2) criminal groups – these aim to infiltrate systems or networks for financial benefits. They deploy phishing, spamming, spyware and malware techniques to steal identity, commit online fraud and engage in extortion; 3) hackers – they explore various cybernetic techniques to break through security defences and to take advantage of security gaps in computer systems and networks. They are motivated by private gain, retribution, persecution, financial benefits or political activism. Hackers devise new types of threats to enjoy recognition in their community; 4) terrorist groups – terrorists mount

cyberattacks to destroy, infiltrate, or take advantage of critical infrastructure to pose a threat to national security, take control over military equipment, disrupt the economy and cause mass casualties; 5) hacktivists – they launch cyberattacks for political reasons, not for financial benefit. They target industries, organisations, or individuals that disagree with their political ideas; 6) "malicious insiders" – these may include employees, external suppliers, contractors, or other business partners that have legal access to business assets and use it for fraudulent purposes to steal or destroy information for financial or personal gain. Malicious insiders usually target businesses, but they also attack state institutions; 7) corporate espionage – corporate spies engage in industrial or business espionage to either gain profit or disrupt the operations of a competitive business by attacking critical infrastructures, stealing company secrets, and gaining unauthorised access. Attacks coming from these individuals may also compromise state security when targeting critical sectors of the economy (StealthLabs, 2020).

Each of these cyberattack sources may employ techniques devised to influence social behaviour and sentiment. With the combination of big data and communication automation through bots and artificial intelligence, it is now possible to distribute information that is both personalised and intended for mass audiences. Data and information theft or extortion, takeover of control over websites and news portals, identity theft, deep fakes – all these can be used to mislead the public, and in extreme cases, to cause social unrest and even armed conflicts. The only effective way to tackle these phenomena is by raising public awareness about their existence.

Reasonable decision-making depends on the individual's ability to analyse available information and to make decisions based on it. In extreme cases, decisions made on the basis of false or incomplete data might cause threats not only for the individual making the decision, but also for the general public and the state.

Researchers from the Max Planck Society have identified four primary challenges facing those responsible for tackling manipulation in the public: 1) user behaviour is often influenced by manipulative website architectures, so-called dark patterns (often leading to undesirable behaviour) – advertisements that appear as website content or navigation guides designed such that a click redirects the user to a website extorting data. These may also include misleading privacy settings, causing the user to provide access to more information than they agreed; 2) AI-operated information architectures do not present information neutrally, but in a personalised manner based on data they gather. This means that two people who enter the same search query in a search engine will probably obtain different results. Such outcome could be helpful when the user is looking for a product or service close to their current location. However, the display of news and political contents based on user preferences can lead to information bubbles, where it is impossible to become familiar with alternative opinions; 3) false and misleading information. Videos and posts with conspiracy theories and unsubstantiated rumours can quickly spread through social media and cause harm – for instance, by discouraging people from

vaccinating through disinformation about vaccines, putting them and other around them at risk of infection; 4) distracting online environments are constantly trying to draw the attention of users. This equally involves push notifications, displays, pop-up advertisements and streams of ever-changing content. The goal is to draw attention from users and make sure to keep them engaged as long as possible. It is a business model and services utilise it, and it is often the case that users spend much more time online than planned without any actual benefits and at the cost of losing time. At the same time, researchers stress that there are no tools to ensure that online manipulations and spread of disinformation are prevented. However, they claim that a combination of intelligent cognitive tools and education in information use with the adoption of anti-manipulation policies by online platforms could significantly reduce the impact of false information on public opinion and human behaviour (Max-Planck-Gesellschaft, 2021).

5 Conclusion

With the widespread access of the Internet and the digitisation of social activities, cyberspace has become the arena for conflicts between states and blocs of states, as well as intelligence wars. One aspect of such conflicts is the so-called information warfare. The deeper the digital skills deficit of the targeted state, the more effective such warfare is. This includes both the public's susceptibility to various types of disinformation and its ability to follow safety rules.

While cyberspace threats cannot be eliminated, it seems that the only non-technical way to reduce vulnerability to them is to educate and raise popular awareness of them. This applies to the general public and all types of cyberspace activities – private, social, professional and political. However, in order for such education to deliver the expected outcomes, it is necessary to improve the digital competencies of the people in charge of it. The reason this is so important is that with the widespread access to the Internet and with rapid technological advancements, existing threats might evolve, or new, unknown ones might emerge. It is likely that in the near future, we will not be able to tell if we are talking to a machine or a human when using instant messaging applications – and this includes not only voice, but also video communication.

The ability to search for and double-check information should be one of the educational outcomes across all educational stages. The public can become more resilient against information warfare once it has a more critical approach to, and can distance itself from, information (especially that which arouses emotions), thus effectively making the state less vulnerable to cyberthreats.

References:

Aronhime, L. & Cocron, A. (2021) *Przeciwdziałanie dezinformacji – wzmocnienie cyfrowej Odporności Sojuszu*, available at: https://www.nato.int/docu/review/pl/articles/2021/08/12/przeciwdzialanie-dezinformacji-wzmocnienie-cyfrowej-odpornosci-sojuszu/index.html (April 20, 2022).

Europa Nu (2021) *Onderwijs en opleiding: basisvaardigheden en digitale vaardigheden essentieel voor onderwijs, werk en leven*, available at: https://www.europa-nu.nl/id/vldphhf4ak7y/nieuws/onderwijs_en_opleiding_basisvaardigheden?ctx=vj5cj4qyvkgm&tab=0 (April 20, 2022).

European Commission (2020) *Education and Training Monitor 2020*, available at: https://op.europa.eu/webpub/eac/education-and-training-monitor-2020/countries/countries.html (April 20, 2022).

Eurostat (2021) *Individuals' level of digital skills*, available at: https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i/default/table?lang=enidw (April 20, 2022).

(2021) *Mensch versus Internet: Was können wir tun, um uns vor Manipulation, Fake News und Co. zu schützen?*, available at: https://nachrichten.idw-online.de/2021/02/12/mensch-versus-internet-was-koennen-wir-tun-um-uns-vor-manipulation-fake-news-und-co-zu-schuetzen/ (April 20, 2022).

Kangasniemi, H. (2020) *Sosiaalisen manipuloinnin avulla yritetään saada ihminen huomaamattaan luovuttamaan arvokkaita tietoja tai rahaa. Kyberrikolliset ovat ottaneet keinon tehokäyttöön ja se koskee meitä kaikkia*, available at: https://elisa.fi/ideat/tunnista-ja-torju-sosiaalinen-manipulointi/ (April 20, 2022).

KPRM (2020) *Kompetencje cyfrowe*, available at: https://www.gov.pl/web/cyfryzacja/kompetencje-cyfrowe (April 20, 2022).

Max-Planck-Gesellschaft (2021) *Selbsthilfe gegen Manipulation im Internet*, available at: https://www.mpg.de/16406549/0211-bild-mensch-versus-internet-was-koennen-wir-tun-um-uns-vor-manipulation-fake-news-und-co-149835-x (April 20, 2022).

Spiegel (2021) *EU muss mehr digitale Kompetenzen fördern*, available at: https://www.bildungsspiegel.de/news/weiterbildung-bildungspolitik/4749-eu-muss-mehr-digitale-kompetenzen-foerdern (April 20, 2022).

StealthLabs (2020) *Cyber Security Threats and Attacks: All You Need to Know*, available at: https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/ (April 20, 2022).

Techrush (2021) *Analyse in Europa: Vielen Erwachsenen fehlt es an Digital-Kompetenz*, available at: https://techrush.de/analyse-in-europa-vielen-erwachsenen-fehlt-es-an-digital-kompetenz/?cookie-state-change=1631368316921 (April 20, 2022).

Tomala, L. (2021) *Kto wierzy w fake newsy? Badacze chcą zwalczać szkodliwe informacje jak epidemie*, available at: https://naukawpolsce.pap.pl/aktualnosci/news%2C86178%2Ckto-wierzy-w-fake-newsy-badacze-chca-zwalczac-szkodliwe-informacje-jak (April 20, 2022).

Activities for Cybersecurity as a Mission of Information Sharing and Analysis Centres

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract Today's environment of cybersecurity threats poses a challenge that has never been greater before, and the need to ensure cybersecurity is particularly notable amidst the COVID-19 pandemic. The increase in the number of sophisticated cyber attacks directed against governments and enterprises – in particular, public entities – has revealed the need to build cybersecurity strategies practically in every sphere of our lives. Organisations therefore need to protect themselves against cyber attacks in which the collected information is at the same time their primary source and target. Due to the increasing need for ensuring cybersecurity, the benefits that can be derived from joint actions seem obvious. However, the key element of such coordinated measures is information sharing and prompt response. Organisations operate better in a situation where threats are identified and described, if they are better informed about the perpetrators and the methods of attacks. Information Sharing and Analysis Centres are one of several tools used with a view to ensuring cybersecurity.

Keywords: • cybersecurity • cyber attack • threat • information

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Dr. Habil., University Professor, Head of the Media Law, War Studies University, Faculty of National Security, Intellectual Property and New Technology Department Institute of Law, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: k.jentkiewicz@akademia.mil.pl, ORCID: 0000-0003-0188-5704.

https://doi.org/10.4335/2022.1.4 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

By design, the Information Sharing and Analysis Centre (ISAC) is a trusted sectoral unit which may provide 24/7 secure operational capability and which sets out the requirements concerning coordination, information sharing and analyses in the event of cybernetic incidents, threats and vulnerabilities in ICT networks. On the one hand, ISAC may serve as a sectoral resource, thanks to which it is possible to collect key information about incidents and issues related to cybersecurity in a given industry, and to identify, communicate, and analyse the potential outcomes of such problems for a given sector. On the other hand, the establishment of ISAC does not necessarily need to entail measures taken only in a given sector. Coordination may refer to joint undertakings or to the achievement of joint objectives related to the need to ensure system-based protection. The common denominator for the activities of partners in the sphere of cybersecurity is often the strategic nature of their services, constituting a crucial point on the map of a critical state infrastructure.

ISAC's mission is first and foremost to increase the sectoral capacity to undertake measures for cybersecurity, respond to threats in the cyberspace, search for vulnerabilities and mitigate the effects of incidents by providing a centralised organisation dealing with the monitoring and dissemination of information. The primary objective is to obtain accurate, useful and relevant critical information whose scope is as useful for cybersecurity as possible. A secondary, but equally important, objective is to maintain the confidentiality of such information, which is deemed significant for cybersecurity by ISAC members. Accordingly, it can be said the ISAC itself constitutes a platform where members can exchange information within their sector, with other organisations, and the government, which means that it is a communication tool and serves as the main communication channel in the sphere of security for a given industry. It ensures the analysis of proper threats, vulnerabilities and incidents. Moreover, it provides access to alerts concerning threats, warnings, guidance, notices and vulnerability analyses to ISAC members.

2 ISACs and critical infrastructure (CI) – the American organisation model

In 1998 B. Clinton's administration issued Presidential Decision Directive 63 (PDD-63) in which the U.S. Government requested that each critical infrastructure sector (in the USA, critical infrastructure sectors include: the chemical sector, commercial facilities sector, critical manufacturing, dams, defence industrial base sector, emergency services, energy sector, financial services, food and agriculture, government facilities, healthcare & public health, Information Technology sector, nuclear reactors, materials and waste sector, transportation systems, and the water and wastewater systems sector) identify sector-specific information to assess a given sector's vulnerability to cyber-attacks or physical attacks, recommend a plan to eliminate significant vulnerabilities, propose a system for identifying and preventing attempted major attacks, and develop a plan for

alerting, containing and rebuffing an attack in progress and reconstitute minimum essential capabilities in the aftermath of an attack. In response to these needs, the owners and operators of key resources of critical infrastructure established ISACs. In 2003, Homeland Security Presidential Directive (HSPD-7) expanded the scope of PDD-63, ordering that the public and private sectors share information about physical and cyber threats, and vulnerabilities with a view to ensuring the protection of critical infrastructure in the USA. Ten years later, in 2013, Presidential Policy Directive 21 (PPD-21) updated the federal approach to critical infrastructure security and resilience by establishing closer links between physical security and cyber security and by strengthening critical infrastructure resilience with three strategic imperatives: 1) to refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience; 2) enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and 3) implement an integration and analysis function to support planning and operations decisions regarding critical infrastructure.

On the same day, President B. Obama issued Executive Order (EO) No. 13636. The document was aimed at improving critical infrastructure cybersecurity by streamlining information sharing between governmental agencies and between the public and the private sector entities, thus increasing the volume, timeliness and quality of cyber threat information. ISACs were established for specific sectors to ensure national security in the protection of critical infrastructure.

ISACs in the USA are used in multiple CI sectors in order to join the efforts of industries and the government, and to ensure measures for quick access to persons affected by cyber-attacks. A lot of these are "inter-sectoral" ISACs (e.g. communications, IT sectors, inter-state ISACs, etc.) that bring together owners of CI or service providers, and operators representing numerous sectors. The key ISACs in the USA include: 1) Financial Services ISAC: The centre has over 4,600 members and 39 partner associations, with an outreach to 99 percent of all banks and credit unions, and covers 85 percent of the securities sector and nearly 50 percent of all insurance firms; 2) Information Technology ISAC: through its members, it reaches 90 percent of all PCs and operational systems, covers 85 percent of all data bases, 85 percent of all routers, and 65 percent of all software safeguards; 3) Communications ISAC: the DHS National Coordinating Center for Communications cooperates with the private sector, including ISACs, in order to ensure 24/7 operational support. Its members include communications equipment and software providers, and it covers 95 percent of all cable lines of communications service providers, 90 percent of all wireless communications service providers, including satellite communications services, and 90 percent of the backbone network of online service providers; 4) Water ISAC: currently provides information about the security of water supply and wastewater companies, and serves over 65 percent of the American population; 5) Multi-State ISAC: covers all 50 states, the District of Columbia, four USA territories and numerous local government authorities. Moreover, MS-ISAC is continuously extending its operations,

and they currently cover all 39,000 municipalities; 6) transport was identified as one of the key sectors, with four existing transport ISACs: a) the Surface Transportation ISAC: In 2002, at the request of the Secretary of Transport, the Association for American Railroads established ST-ISAC. ST-ISAC serves 95 percent of the total North American rail infrastructure; b) Over the Road Bus ISAC: supported by ST-ISAC, the American Bus Association initiated the operations of the OTRB ISAC in 2013. ABA provides security alerts and password-protected information in the relevant section of their website; c) Public Transportation ISAC (PT-ISAC): The American Public Transportation Association was appointed by the U.S. Department of Transportation as the sector coordinator for the public transport industry in the United States. To this end, APTA established PT-ISAC. APTA members provide services to over 90 percent of all public transport users in the USA and Canada; d) Maritime ISAC: This ISAC is a non-profit organisation sponsored and managed by the Maritime Security Council. The Maritime ISAC cooperates with the U.S. and international maritime shipping, seaport and government regulatory oversight communities. It deals with collecting and analysing proprietary data (e.g., stowaway rates and locations, drug seizures overseas, terrorist threats etc.), which it then disseminates to participating industry and government constituents; 7) Retail ISAC: The Retail Cyber Intelligence Sharing Center acts as a platform for retailers where they can exchange information on threats and leading practices, at the same time improving the security of retail networks and protecting consumer data. The analysts of the Retail ISAC process and collect real-time information on cyber threats (including new types of malware, the operations of underground criminal forums or potential software vulnerabilities). It also provides anonymised information to the federal government and law enforcement bodies, such as the DHS, Secret Service or the Federal Bureau of Investigation (Goodwin, Nicholas, 2015).

3 The cooperation of ISACs with other entities

The analysis of American ISACs reveals close links between government agencies and ISACs in the sphere of counteracting cyber-attacks. The transportation sector is one example of this. Along with the update of the national approach to the security and resilience of critical infrastructure, 16 critical infrastructure sectors were identified, and the related sector-specific federal agencies were appointed. The Department of Transportation is responsible for providing technical support to CI owners and operators, and for facilitating access to, and exchange of, information necessary to enhance and protect transportation security. DHS manages the National Cybersecurity and Communications Integration Center, which is a centre responsible for coordinating emergency information about cyberspace and communications across the country, operating 24/7, engaging in cooperation state and local authorities, intelligence communities, law enforcement bodies and the private sector. The Operational Control and Emergency Communications Center is a centralised institution whose objectives are to ensure cybersecurity and to raise the awareness of threats in the sphere of

communications, vulnerabilities, hacking, incidents, as well as mitigating and recovery measures.

In 2011 DHS launched an information sharing and cooperation programme in respect of the cyberspace in order to raise awareness within all critical infrastructure sectors through a close and timely exchange of information about cybernetic threats and direct analytical exchange. The programme covers governmental organisations, ISACs and other CI owners and operators through the development of a mechanism by which private sector partners would be able to share data directly with the government via an inter-sectoral portal. Fully integrated divisions allow a holistic approach to cybersecurity and communications issues at the operational level. The sectoral partnership model is set out in the National Infrastructure Protection Plan (NIPP). The model encourages CI owners and operators to establish Coordinating Councils which are to: 1) represent principal entry points for the government to collaborate with the sector with a view to solving problems; 2) serve as a strategic communication and coordination mechanism between owners, operators and suppliers of IC, and, as appropriate, with the government during emerging threats or response and recovery operations; 3) identify, implement and support appropriate information-sharing capabilities and mechanisms in sectors; 4) facilitate inclusive organisation and coordination of the sector's policy development regarding critical infrastructure security and resilience planning and preparedness, exercises and training, public awareness and associated implementation activities and requirements; 5) advise on the integration of federal, state local and regional planning with private sector initiatives; and 6) provide input to the government on sector R&D efforts.

Government Coordinating Councils cooperate with ISACs. Their tasks include: 1) the provision of inter-agency strategic communications and coordination at the sectoral level through partnership with DHS, Sector-Specific Agency and other supporting agencies across various levels of government; 2) participation in planning efforts related to the revision of the National Plan and the development, implementation and revision of Sectoral Plans; 3) coordination of strategic communications and discussion and resolution of issues among government entities within the sector; and 4) coordination of, and support for, the efforts to plan, implement and execute the Nation's critical infrastructure security and resilience mission.

One of the strengths of the ISAC "system" is the exchange of data and experience with other related ISACs. The National Council of ISACs (NCI) is one of several such information sharing mechanisms. Formerly known as the ISAC Council, the NCI is a group of volunteer representatives of ISACs who meet to develop trusted relationships between sectors and to address common issues. Each ISAC appoints four representatives to the Council. The mission of NCI is to increase physical security and cybersecurity of national critical infrastructure through establishing and maintaining a framework for valuable interaction between the ISACs and the government. The NCI holds monthly meetings via teleconference and quarterly on-site meetings to discuss current issues. The

NCI also sponsors the annual Critical Infrastructure Protection Congress to bring together the critical infrastructure community for networking, learning and addressing issues of concern to stakeholders. The mission of the Partnership for Critical Infrastructure Security (PCIS) is to coordinate common CI cross-sector initiatives that promote public and private efforts to help ensure secure, safe, reliable, and resilient critical infrastructure services.

Some information sharing programmes, in particular in the private sector, operate via local companies, universities and experts who discuss common threats and vulnerabilities.

In the United States, non-profit programmes, such as the Bay Area Chief Security Office Council, and the Massachusetts Advanced Cyber Security Center, are examples of regional information exchange organisations. The Federal Bureau of Investigation (FBI) also has developed the InfraGard, a regional public-private information-sharing hub.
Numerous information exchange schemes at the national level, both voluntary and mandatory, include all information-sharing participants and influence them. The inherent role of national governments in the sphere of legal regulations and security suggests the need for national information exchange programmes. In the United States, most proposals from the Congress and the executive branch are centred around participation in new national-level information sharing programmes.

Cyberthreats usually have an international reach, so information sharing participants might wish to communicate within the international agenda. For governments, such disclosure may be problematic, as the provision of sensitive or even confidential information can only occur between close allies. As a result, the efforts aimed at the establishment of international information sharing schemes in which governments participate have not been successful.

The analysis of the American ISAC model shows that mitigating cybersecurity risks increasingly depends on information sharing and cooperation between a wide range of entities, with the use of numerous diverse collaboration models, methods and instruments. The design of successful information-exchange mechanisms is not an easy endeavour, as it requires continuous engagement, trust and a clear sense of values shared by entities participating in a given project. The key element of ensuring support related to information sharing is the coordination of activities, in particular, those taken by public and private organisations. Nonetheless, it is crucial to build such information-sharing and cooperation tools among entities of substantial strategic importance for the state in the public-sector area.

4 ISAC – the European model

European ISACs differ from their American counterparts in terms of dynamics and characteristics. First of all, European ISACs build on the experience of older organisations from across the Atlantic. Secondly, European ISACs are very much distinct from the American ones, which results from cultural differences – in the USA, businesses are expected to take care of themselves, while in Europe it is expected that the state ensures cybersecurity in each sector, while the majority of key public tasks are performed in full by the public sector.

European ISACs focus on building partnerships and trust between their members. They are very industry-oriented, but there are also high expectations about governmental support – not in terms of financing, but rather in the substantive area through sharing specialist knowledge (combating cybercrime, sharing industry-relevant information). The participation of public administration increases the effectiveness of ISACs. Moreover, it proves the respect and support for market needs on the part of the public sector, in political and strategic terms (for example, such need is indicated in the Directive on security of network and information systems and in the GDPR).

The development of the ISAC ecosystem in Europe depends on the cultural conditions of individual members and the general level of trust between public and private entities – if a public-private partnership (PPP) is involved. Therefore, in countries where the trust is insufficient, it is worth starting from developing appropriate PPP structures, and then transforming them into an ISAC. This is owing to the fact that the exchange of information about incidents is very demanding, and the level of trust between participating entities is of great importance here. As key services require the establishment of this type of organisations to enhance cybersecurity, ISACs bringing together only public sector partners are also needed, if not indispensable.

It is worth noting here that international or large enterprises operating in the cybersecurity sector (in Europe) are usually not involved in ISACs. This is mainly due to the insufficient trust of ISAC members in such companies, which is based on the belief that they might use the provided information and knowledge to advance their own business. That is why the benefits that might be derived from such participation should be explored beforehand. There are three roles in an ISAC – moderator, member and partner. The moderator (leader) is an entity which defines the logistics of the group (it assumes the function of a secretariat); a member is an organisation which actively discloses or receives information; and a partner is an entity which may take part in dedicated sessions, usually aimed at providing specified information (research data) or discussing a specific topic (e.g. transposition of a directive to national law).

5 Conclusions

Cyberthreats and cyber attacks are not only a technological risk, but also a business risk. Therefore, the cybersecurity function should have sufficient independence and significance. This might help ensure the proper consideration of decisions related to risk management that are not affected by other issues and IT limitations, or overshadowed by them. If cybersecurity is part of IT, it might lack sufficient visibility and links with the actual services. Enterprises should therefore consider specific measures with a view to establishing links between services, risk partners and cybersecurity. This could be achieved through the creation of steering committees within the framework of ISACs. Such measures could also facilitate the alignment of cybersecurity measures with future business plans.

The COVID-19 pandemic has significantly disrupted the operations of institutions and their functioning worldwide. Remote work has gained popularity, and as a result, the number of videoconferences and team collaboration applications have rapidly increased. In a recent report prepared by Deloitte, it was found that many financial institutions were evaluating permanent remote work for at least part of their workforce. Indeed, based on conversations with industry leaders, some companies are considering remote work for 30% or more of their employees on a more permanent basis. Cybersecurity organisations will need to quickly adapt to this new operating environment by implementing enhanced controls and endpoint protection technologies so as to exert greater control over end-user devices. Companies should, hence, consider increasing training and awareness activities, focusing on remote etiquette for work-from-home environments. Such experience should be the subject of information exchange as part of ISACs (Bernard, Nicholson, 2020).

References:

Bernard, J. & Nicholson, M. (2020) *Reshaping the cybersecurity landscape How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions*, available at: https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html (March 15, 2022).

Goodwin, C. & Nicholas, J.P. (2015) *A framework for cybersecurity information sharing and risk reduction*, available at: C:/Users/48692/Downloads/Framework_for_Cybersecurity_Info_Sharing%20(1).pdf (March 15, 2022).

Information Protection in Cyberspace a Factor in National Security

KRZYSZTOF BOJARSKI

Abstract National security is a very broad issue and includes a number of factors that may affect the security situation. In addition to the traditionally considered, especially of a military nature, nowadays attention is also drawn to other elements, among which those related to national security in cyberspace are of particular importance, and in this respect, especially the security of information, in particular, of classified information. Ensuring national security in this regard is currently becoming a key challenge for the state's functioning and development. Therefore, mechanisms, procedures and structures are being put in place to safeguard this security at different levels of state function.

Keywords: • national security • cyberspace • cybersecurity • classified information

CORRESPONDENCE ADDRESS: Krzysztof Bojarski, Ph.D., Faculty of Security, Marshall Józef Piłsudski Higher School of Safety and Security in Warsaw, Zakroczymska Street 13, 00-225 Warsaw, Poland, e-mail: k.bojarski@wsbio.waw.pl, ORCID: 0000-0002-0729-5759.

https://doi.org/10.4335/2022.1.5 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Security, in its broad sense, is nowadays a ubiquitous notion, considered in various scopes and in relation to various values. One of the key issues of security is national security. This is because in any country, its national security affects the security of every citizen of that state, their lives and development. Hence it must be taken seriously. Indeed, Article 5 of the Constitution of the Republic of Poland of 2 April 1997 (consolidated text, Polish Journal of Laws 1997, No. 78, item 483, as amended) states that "the Republic of Poland shall safeguard the independence and integrity of its territory and ensure the freedoms and rights of persons and citizens, the security of the citizens (...)."

Thus, in one of the first articles of the Constitution, the legislators emphasise issues relating to territorial independence and integrity, and the security of citizens. Independence means, of course, the separate state existence of the Republic, as well as the existence of the Polish state within its present boundaries, while sovereignty is understood as the ability of the state to decide and act independently about all matters concerning it. However, national security is not only about independence and the associated aspect of defending that independence alone, as the concept of national security has evolved considerably over the years. It is true that the traditional approach pays particular attention to the military aspect, and to the absence of threats in this respect. Therefore, in this sense, the fundamental values to be protected include territorial integrity, political independence or even the survival of the state or nation. Of course, these are extremely important aspects of national security, but they are not of sole significance. Today, many other factors are also indicated which influence this security, and at the same time often pose a serious threat to it. These factors include, for example, the destabilisation of the state system, poorly functioning economic and social mechanisms, social conflicts, natural disasters, illegal migration, organised crime, terrorism, and, in recent times in particular, special attention should be paid to threats to the state occurring in cyberspace and the related information domain. Thus, national security is shaped by a number of often interrelated factors that can lead, when significantly intensified, to the destabilisation of the state and, consequently, to the collapse of the state understood as the inability of the central government to perform its basic functions over the entire territory of the state (Bojarski, 2017: 26-27).

2 Cyberspace and cybersecurity – definitional attempt

The starting point for further consideration of the subject in question is cyberspace and its definition, which is provided in Article 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 the Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Polish Journal of Laws of 2017, item 1932) in the wording which determines that cyberspace is understood as space for the processing and exchanging of information created by ICT systems, as defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing

Public Tasks (consolidated text, Polish Journal of Laws of 2021, item 670), including the links between them and relations with the users. Thus, cyberspace is the information space where the processing and distributing of information and messages is carried out. It consists of both ICT networks and systems, and the relationships between them and users (Kowalewski, 2014: 24). Cyberspace can be at the same time identified as an area – an electronic domain – used for the distribution of information, which has an interstate form and consists of the sum of activities carried out by the user (Wasilewski, 2013: 231). Analysing the term itself in even more detail, it should be noted that the prefix "cyber" refers to the use of new information and communication technologies, as well as to the development of e.g. economy, culture or knowledge based on these technologies in a broad sense. The basic element of the term indicates a space that is constantly expanding and evolving as a result of continuous changes based on the ingenuity and participation of users themselves. Therefore, cyberspace obviously requires hardware, software and information systems, but it is also co-created by human behaviour captured through digital networks. All these interactions are a rich set reflecting the positive as well as the negative sides of human nature, ranging from cyberautocreation to criminal activities, also leading to terrorist acts and possible cyber conflicts. It can therefore be concluded that the main characteristics of cyberspace are the absence of borders, dynamic processes and phenomena and the anonymity of users. This situation makes public institutions with their domain in cyberspace vulnerable to intrusion, whether by individuals, organised groups or hostile states (Górka, 2018: 33-34).

This therefore raises the question of cybersecurity – what it is and how it is understood. The definition of cybersecurity is contained in the Act on the National Cybersecurity System of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369) – the Act is hereinafter referred to as the NCSA – according to which cybersecurity is the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems (Article 2(4) of the NCSA). This definition is linked to the definition of the concept of an incident and its various types, which are also defined in the NCSA (Article 2(5-9) and according to which: incident – means an event which has, or may have, an adverse impact on cybersecurity; critical incident – means an incident resulting in significant damage to public security or order, international interests, economic interests, operation of public institutions, civil rights and freedoms or human life and health, classified by the competent CSIRT MON (Computer Security Incident Response Team operating on a national level, managed by the Minister of National Defence), CSIRT NASK (Computer Security Incident Response Team operating on a national level, managed by the Research and Academic Computer Network – National Research Institute) or CSIRT GOV (Computer Security Incident Response Team operating on a national level, managed by the Head of the Internal Security Agency); serious incident – is defined as an incident which causes, or may cause, a serious reduction in the quality, or an interruption of the continuity, of a critical service; significant incident – means an incident which has a significant impact on the provision of a digital service within the meaning of Article 4 of Commission Implementing Regulation (EU) 2018/151

of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ EU L 26, p. 48); incident in a public entity – is an incident which causes, or may cause, a reduction in the quality of, or an interruption to, the performance of a public task carried out by a public entity, as referred to in Article 4(7) to (15) of the NCSA.

Cybersecurity is also addressed by the Cybersecurity Strategy for 2019-2024 (Official Gazette of 2019, item 1037), hereinafter referred to as the Cybersecurity Strategy. First of all, it is worth mentioning a few words about the document itself – namely, that it replaced the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022, and was introduced by a resolution of the Council of Ministers. Moreover, it directly affects government administration bodies, and indirectly, after the adoption of generally applicable laws on the initiative of the Council of Ministers, other public authority bodies, as well as entrepreneurs and citizens. The main motive of this document is to define strategic objectives and appropriate political and regulatory measures aimed at achieving a high level of cybersecurity, i.e. primarily to ensure the resilience of the information systems of operators of essential services, critical infrastructure operators, digital service providers and public administration to cyberthreats, as well as to increase the level of information protection in information systems through standardisation of security features. As a result, the implementation of the strategic objectives is expected to influence the improvement of national security, increase the effectiveness of law enforcement agencies and judicial authorities in detecting and combating cybercrimes, as well as hybrid (including terrorist activities) and espionage activities in cyberspace. Therefore, we can conclude that the main objective of this strategy is to increase the level of resilience to cyberthreats and to enhance the level of information protection in the public, military and private sectors, as well as to promote knowledge and good practices to enable citizens to better protect their information (Cybersecurity Strategy: 8-10).

It must be stressed that cyberspace has been shaped primarily by the process of integration of basic forms of information transmission and interpretation (Marczyk, 2018: 60), which emphasizes the importance of user behaviour from a cybersecurity perspective. Therefore, it seems that activities related to the promotion of knowledge and education in the field of cybersecurity are a prerequisite for the success of information protection in cyberspace, because it is well-known that humans are the weakest link here. For this reason, according to this strategy, education about cybersecurity should be available at the earliest possible stage of access to digital services – preferably before entering the digital world. In practice it is often required at the stage of early childhood education. In this respect, it is advisable that, in cooperation with non-governmental organisations, the private sector and academic centres, the public administration carry out systemic actions to sensitise society to the risks of cyberspace, as well as educational actions in the field

of rights and freedoms in the digital environment and the rights of persons who are victims of cyberattacks and suffer damage as a result of violations of network security.

In the context of the growing number of threats aimed at exerting a specific influence on society, as well as bearing in mind the consequences of the deliberate use of social engineering tools for manipulative activities in the form of, among others, disinformation campaigns or inspiration or disintegration activities, it is necessary to implement systemic actions enabling the development of citizens' awareness in the context of verifying the authenticity of information and responding to attempts to disrupt it (Cybersecurity Strategy, 2019: 26). Indeed, it is not without a reason that the 21st century is called the century of the information society, which emphasises the important role of information and communication systems existing within a given society and determining its specific features as compared to other types of societies. Such a society consists not only of information and ICT means, but also of humans and their needs, the economy, the state and the environment. It is the development of ICT means in processing and collecting information, as well as communication means in sending and receiving information that is responsible for the establishment of the information society (Krztoń, 2015: 101-102) and the related key role of information and its protection.

3 Information and information security

Information is a term which is ambiguous and difficult to define. Although many different definitions can be found in the literature on the subject, it can be assumed, according to the Polish language dictionary, that information is, among other notions, what has been said or written about someone or something, also the communication of something, as well as data processed by a computer (https://sjp.pwn.pl/sjp/informacja;2466189.html). Information is a key factor influencing decision-making in all areas of life. The basis of information is data, which must be understandable and, moreover, should contain an element of novelty for the recipient. However, when defining information in the context of an information system, it is emphasised that information is what changes and supports understanding, while data is the input of the communication channel, as data is tangible and consists of numbers, words, phone calls, etc. Data becomes information when people use it to better understand specific issues. As a result, information systems should provide information rather than data. Information in any organisation, including the state, is the basis for building the knowledge of all people involved in the process of acquiring and using it. By shaping the awareness of the phenomena occurring in the organisation itself and in its environment, information makes it possible to adapt to the changing reality, as well as to transform it to facilitate the more efficient functioning, for example, of the state as the most universal organisation. Furthermore, it is due to information that it is possible to become aware of existing problems and then to begin the search for solutions (Grabowski, Zając, 2009: 104).

Nowadays, information in the virtual world is of particular importance. This is because it is the most important element of cyberspace, being generated from data which, when processed, commented and disseminated, creates a new dimension of reality.

Today more than ever, a new facet of information is revealed – namely, in the modern world information it is treated as a commodity, which, like any other good, can be bought and sold. As a result, the growing importance and significance of information in both the economic and national security fields is gradually but continuously increasing its price. It is already a truism today to say that those who have information have power. Therefore, it is not surprising that adequate cybersecurity has become a priority for many governments in recent years (Cyfrowa Polska, 2019: 3), since thanks to the global Internet, all who are interested have access to almost the entire world. In addition to the obvious benefits, however, this also has its dark side, because it entails a new threat to national security, which takes the form of uncontrolled leakage of information of not only economic, political, but even strategic importance.

Such a threat requires effective action to eliminate or minimise it. Therefore, there is a need for constant monitoring of the situation, and thus for the establishment of services, institutions or organisations which, on the basis of appropriate legal regulations, will ensure the security of the state in this field of its functioning. Similarly to other countries, Poland is also susceptible to the threat of information leakage, which may be the result of improper management of information resources or deliberate action by intelligence and special services of other countries, or even terrorist organisations hostile to Poland and its domestic and foreign policy. Particularly important and sought-after is not only military and national defence data, but also data relating to business activity, technology and scientific research, and in fact any information that may contribute to the competitive advantage of another country or organisation. Therefore, in response to a new threat, in order to ensure the security of information that is particularly important to the state, all countries establish properly prepared and trained services whose task is to constantly monitor information security and eliminate or limit its leakage. In the functioning of the state, the efficiency of governing bodies is of utmost importance, which is mainly related to the speed and accuracy of decisions, and this in turn depends on the availability of a large amount of reliable and detailed information in a given area, so security management must be organised in such a way that information is easily accessible to authorised persons and at the same time protected from unauthorised use by outsiders who may act to the detriment of the state (Machura, 2013: 156-157). This, of course, also, and perhaps above all, requires appropriate legal regulations.

The principal legal act relating to this issue is the Act of 5 August 2010 on the Protection of Classified Information (Polish Journal of Laws of 2019, item 742) – the Act is hereinafter referred to as the APCI. The provisions set out in this Act govern the standards for the protection of classified information, the classification of classified information, the preparation of its protection, as well as the standards for the use of physical, personnel and ICT security measures (Wojciechowska-Filipek, Ciekanowski, 2019: 195).

According to this legal act, classified information is considered to be 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 (Article 1(1) of the APCI). Classified information may be made available only to a person providing a guarantee of confidentiality and only to the extent necessary for the performance of their work or service at the position held or for the performance of commissioned activities (Article 4(1) of the APCI).

Proper management of access to classified information requires its appropriate classification, and in accordance with the APCI, it may be assigned one of four secrecy clauses, the common denominator of which is the fact that its disclosure may have negative consequences for national security. Therefore, according to Article 5(1) of the APCI, classified information shall be marked as "top secret" if its unauthorised disclosure causes exceptionally serious damage to the Republic of Poland by: 1) threatening the independence, sovereignty or territorial integrity of the Republic of Poland; 2) posing a threat to the internal security or constitutional order of the Republic of Poland; 3) posing a threat to the alliances or the international position of the Republic of Poland; 4) weakening the defence readiness of the Republic of Poland; 5) that fact that it will or may lead to the identification of officers, soldiers or employees of the services responsible for the performance of intelligence or counterintelligence tasks, and who perform operational and exploratory activities, if this endangers the security of the activities performed or may lead to the identification of persons assisting them in this respect; 6) the fact that it will or may endanger the life or health of officers, soldiers or employees who perform operational and exploratory activities, or persons assisting them in this respect; 7) the fact that it will or may endanger the life or health of crown witnesses or persons closest to them, persons who have been granted protection and assistance measures provided for in the Act of 28 November 2014 on the protection and assistance for the victim and the witness (Polish Journal of Laws of 2015, item 21), or witnesses referred to in Article 184 of the Act of 6 June 1997 of the Code of Criminal Proceedings, (consolidated text, Polish Journal of Laws of 2021, item 534), or persons closest to them.

In turn, classified information is classified as "secret" if its unauthorised disclosure causes serious damage to the Republic of Poland by: 1) making it impossible to perform tasks related to the protection of the sovereignty or constitutional order of the Republic of Poland; 2) deteriorating the relations of the Republic of Poland with other states or international organisations; 3) disrupting the defence preparations of the state or the functioning of the Armed Forces of the Republic of Poland; 4) hindering the performance of operational and exploratory activities carried out in order to ensure the security of the state or the pursuit of perpetrators of crimes by services or institutions authorised to do so; 5) significantly disrupting the functioning of law enforcement agencies and judicial authorities; 6) bringing about a considerable loss to the economic interests of the Republic of Poland.

Classified information may also be classified as "confidential" if its unauthorised disclosure causes damage to the Republic of Poland by: 1) hindering the current foreign policy of the Republic of Poland; 2) hindering the implementation of defence undertakings or adversely affecting the combat capability of the Armed Forces of the Republic of Poland; 3) disrupting public order or endangering the security of citizens; 4) hindering the performance of tasks by services or institutions responsible for protecting the security or fundamental interests of the Republic of Poland; 5) hindering the performance of tasks by services or institutions responsible for the protection of public order, security of citizens or prosecution of perpetrators of crimes and fiscal offences, as well as judicial authorities; 6) threatening the stability of the financial system of the Republic of Poland; 7) adversely affecting the functioning of the national economy.

Finally, classified information is classified as "proprietary" if it has not been assigned a higher security classification, and its unauthorised disclosure may have a harmful effect on the performance of tasks in the field of national defence, foreign policy, public security, observance of citizens' rights and freedoms, judicial authorities or the economic interests of the Republic of Poland by public authorities or other organisational units.

Classified information assigned a specific security classification should be protected in accordance with the criteria specified in a given classification. The security classification of documents should be assigned by the person authorised to sign them. Classified information with a security classification may be disclosed only to an authorised person holding an appropriate security clearance, and who had undergone training on the protection of classified information. Information is made available only to the extent necessary for the performance of duties on a given position. The processing of classified information obligatorily takes place in conditions that prevent its unlawful disclosure, e.g. in classified registry offices or other places that can meet the requirements set out in the Act, as well as in secondary legislation, related to the physical protection and security of ICT systems (Wojciechowska-Filipek, Ciekanowski, 2019: 200). The issue of security of ICT systems, which is key from the point of view of information security in cyberspace, will be discussed further below.

At this point, however, it is worth presenting the conditions for marking materials with specific classifications, which are set out in the Regulation of the Prime Minister of 22 December 2011 on the manner of marking materials and affixing security classifications on them (Polish Journal of Laws of 2011, No. 288, item 1692) – the Regulation is hereinafter referred to as the RMMCL. Without going into too much detail, it is necessary to mention several basic principles related to marking materials with security classifications. First of all, in accordance with § 3 of the RMMCL, the material must be marked clearly and in full with the security classification. Where different parts of the material have been given different security classifications, or where some parts are unclassified, the separate parts must be marked with the relevant security classification indicated in full or with the word "unclassified". The parts of the material containing text or images shall be separated by appropriate marking before and after the text or images.

If different parts of the material have been given different security classifications, the material shall be marked with a security classification at least equal to the highest security classification given to that part of the material.

Regarding the symbols used for the individual security classifications, in accordance with § 4 of the RMMCL, the following symbols for security classifications apply: 1) "00" – for "top secret" classification; 2) "0" – for "secret" classification; 3) "C" – for "confidential" classification; 4) "P" – for "proprietary" classification. From a cybersecurity point of view, the handling of electronic documents is particularly important, so, for example, according to § 6 (1) of the RMMCL, an electronic document must be marked in such a way that its specification contains the following information: 1) the security classification; 2) the letter and number reference; 3) the name of the unit or organisational unit; 4) the document registration date; 5) in the case of a document processed as correspondence, the indication of the addressees by stating their full names or the names of their positions; 6) the security classifications of any annexes, together with their registration numbers; 7) the position, full name or other indication of the person authorised to sign the document; 8) the full name or other indication of the person preparing the document; 9) the name given to the document or the indication of what the document relates to.

In addition, in relation to threats to the security of classified information in cyberspace, ICT security is extremely important. The basic requirements in this respect are set out in the Regulation of the Prime Minister of 20 July 2011 on basic requirements for ICT security (Polish Journal of Laws of 2011, No. 159, item 948) – the Regulation is hereinafter referred to as the RRIS. § 5 of the RRIS states that the security of classified information processed in an ICT system shall be ensured by implementing a consistent set of safeguards to ensure the confidentiality, integrity and availability of that information. This objective shall be achieved by: 1) subjecting an ICT system to the risk management process for the security of classified information processed in the ICT system; 2) limiting trust, consisting in treating other ICT systems as potential sources of threats and implementing in the ICT system safeguards controlling the exchange of information with those ICT systems; 3) implementing multi-level protection within the ICT system, consisting in the application of safeguards on as many different levels of organisation of protection of the ICT system as possible - in order to limit the occurrence of cases in which a breach of a single safeguard results in a violation of the aforementioned objective; 4) performing periodic security tests; 5) limiting authorisations, by way of giving users of an ICT system only the authorisations necessary to perform their work; 6) minimising functionality by way of installing, activating and using in an ICT system only the functions, communication protocols and services necessary for the correct performance of tasks for which the ICT system is intended.

Moreover, § 6 of the RRIS stipulates that in order to ensure protection against unauthorised access to an ICT system: 1) the conditions and manner of assigning users authorisations to work in an ICT system shall be determined; 2) information and materials

enabling access to an ICT system shall be protected; 3) elements of an ICT system which are important for its security shall be protected and implemented in a manner ensuring the possibility of detecting unauthorised changes or attempts to introduce them. Also, according to § 7 of the RRIS, before allowing persons to work in an ICT system, the head of an organisational unit shall ensure that they have been trained in the field of ICT security and have been familiarised with procedures for secure operation within the scope applicable to them. In order to prevent the loss of confidentiality of classified information due to electromagnetic compromising emanation from system components, electromagnetic protection measures must be applied in an ICT system processing classified information with the "confidential" classification or above, based on the results of a risk assessment for the security of classified information, taking into account the recommendations.

Beyond the aforementioned, a similar approach is taken in relation to preventing the loss of availability of classified information processed in ICT equipment as a result of interference with its operation by means of emanation or high-power electromagnetic pulses, by employing electromagnetic protection measures selected on the basis of the results of a risk assessment for the security of classified information (§ 8(1) of the RRIS). However, in order to ensure availability of resources in an ICT system, the following shall be established: 1) principles of creating and storing backup copies; 2) procedures for handling crisis situations, including cases of failure of ICT system components; 3) procedures for monitoring the technical condition of an ICT system. Depending on the needs and results of a risk assessment for the security of classified information, alternative telecommunication links, alternative equipment or emergency power supply shall be used in particular to ensure the availability of the resources of an ICT system (§ 9(1) of the RRIS). Depending on the needs and the results of a risk assessment for the security of classified information, data transmissions between ICT system components shall be protected against detection, interception or interference.

Furthermore, the confidentiality of classified information communicated in the form of transmission outside protection zones shall be ensured by the use of encryption devices or tools certified in accordance with Article 50(2) of the APCI or approved under Article 50(7) of the APCI, appropriate to the security classification of the information communicated. In particularly justified cases, taking into account the results of a risk assessment for the security of classified information, the encryption protection measures referred to above may be supplemented or replaced by safeguards other than encryption (§ 10 of the RRIS). To the extent necessary to ensure review, analysis and provision of evidence of actions violating the security of classified information, records of events shall be created and stored for an ICT system processing classified information, and their confidentiality, integrity and availability shall be ensured (§ 11of the RRIS). In addition, an ICT system shall be provided with mechanisms or procedures preventing ICT security incidents, including protection against malicious software, as well as enabling the quickest possible detection of ICT security incidents and ensuring that appropriate persons are immediately informed of a detected incident (§ 12 of the RRIS).

The head of the organisational unit in which classified information is processed is responsible for the protection of classified information. He/she is charged with, in particular, organising and ensuring the functioning of such protection. Therefore, a classified information security officer employed by the head of the organisational unit reports directly to the head of the organisational unit and is tasked with ensuring compliance with the provisions on the protection of classified information. Such officers are required to have: 1) Polish citizenship; 2) higher education; 3) an appropriate security clearance issued by the Internal Security Agency (ISA) or the Military Counterintelligence Service (MCS), as well as by the former Office for State Protection or the former Military Information Services; 4) a certificate of classified information protection training conducted by the ISA or the MCS, as well as by the former Military Information Services. The head of the organisational unit may also employ a deputy or deputies of the security officer, provided that such persons fulfil the conditions referred to above (Article 14(1) to (4) of the APCI).

On the national level, the ISA and the MCS perform a special role in the protection of classified information. As provided for in Article 10(1) of the APCI, the ISA and the MCS supervising the functioning of the classified information protection system in organisational units within their competence set out in the aforementioned act: 1) control the protection of classified information and the observance of the provisions in force in this respect; 2) perform tasks in the field of security of ICT systems; 3) conduct verifying proceedings, control verifying proceedings and industrial security proceedings; 4) ensure the protection of classified information exchanged between the Republic of Poland and other states or international organisations; 5) provide advisory services and conduct training in the protection of classified information. The Head of the ISA performs the function of a national security authority and, to the extent necessary for the performance of this function, the Head of the ISA or officers of the ISA authorised by him, and the Head of the MCS or soldiers or officers of the MCS authorised by him have the right to: 1) inspect documents relating to the protection of international classified information; 2) enter premises and facilities intended for the processing of international classified information; 3) access ICT systems intended for the processing of international classified information; 4) obtain explanations and information relating to the protection of international classified information (Article 11(1) to (4) of the APCI).

4 Conclusion

Cybersecurity, and the security of classified information, becomes all the more important, the more we realise that today actions below the threshold of war are and will continue to be an important policy measure, enabling both state and non-state actors to achieve their objectives. Therefore, information security in cyberspace is now becoming one of the key areas of national security, both in relation to the structures of the state, its citizens and their activities. This is, of course, among others, a consequence of the rapid progress in digital technologies, which is at the same time a challenge for the state, which is forced

to join the technological race in this area (National Security Strategy of the Republic of Poland, 2020: 7-8). Accordingly, the importance of cyberspace for the functioning of the state needs to be constantly emphasised, as actions taken in cyberspace have a direct impact on all key components of the state, and threats to the security of classified information are particularly serious in this respect and should be given increased attention (Biernacik, 2018: 13). It seems that awareness of these threats and of the damage that may be caused as a result of the unauthorised disclosure of classified information is growing, among those in power and among public administration employees, but also among average citizens. However, without appropriate knowledge in this area, strict observance of procedures, as well as adequate ICT infrastructure, we will continue to be exposed to a real danger resulting from activities taking place in cyberspace, because nowadays, and probably even more so in the future, both dimensions, the real and the virtual, are and will remain in an even greater and closer relationship.

References:

Biernacik, B. (2018) Nauka i najnowsze narzędzia informatyczne w służbie bezpieczeństwa cyberprzestrzeni – piątego wymiaru walki zbrojnej, In: Roman, Ł., Krassowski, K., Sagan, S. & Wróblewski, D. (eds) *Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń* (Józefów: Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie), pp. 9-39.

Bojarski, K. (2017) *Współdziałanie administracji publicznej z organizacjami pozarządowymi w sferze bezpieczeństwa wewnętrznego w ujęciu administracyjno-prawnym* (Warszawa-Nisko: Wydawnictwo Wyższej Szkoły Bezpieczeństwa i Ochrony im. Marszałka Józefa Piłsudskiego w Warszawie).

Cyfrowa Polska (2019) *Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań* (Warszawa), available at: https://cyfrowapolska.org/wp-content/uploads/2019/01/Raport_cyberbezpiecze%C5%84stwo_2019.pdf (April 12, 2022).

Górka, M. (2018) Cyberbezpieczeństwo jako wyzwania dla państwa i społeczeństwa, In: Dębowski, T. (ed.) *Cyberbezpieczeństwo wyzwaniem XXI wieku* (Łódź-Wrocław: ArchaeAgraph Wydawnictwo Naukowe), pp. 31-50.

Grabowski, M. & Zając, A. (2009) Dane, informacja, wiedza – próba definicji, *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie*, 798, pp. 99-116.

Kowalewski, J. & Kowalewski, M. (2014) Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa, *Telekomunikacja i Techniki Informacyjne*, 1-2, pp. 24-32.

Krztoń, W. (2015) XXI wiek – wiekiem społeczeństwa informacyjnego, *Modern Management Review*, 3, pp. 101-112.

Machura, E. (2013) Informacja i jej znaczenie we współczesnym świecie w kontekście ochrony informacji niejawnych w Polsce, *Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej*, 1, pp. 155-167.

Marczyk, M. (2018) Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, *Przegląd Teleinformatyczny*, 1-2, pp. 59-72.

Słownik języka polskiego, available at: https://sjp.pwn.pl/sjp/informacja;2466189.html (April 12, 2022).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2020), available at: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf (April 12, 2022).

Cybersecurity Strategy for 2019-2024 (Official Gazette of 2019, item 1037).

Wasilewski, J. (2013) Zarys definicji cyberprzestrzeni, *Przegląd Bezpieczeństwa Wewnętrznego*, 5, pp. 225-234.

Wojciechowska-Filipek, S. & Ciekanowski, Z. (2019) *Bepieczeństwo funkcjonowania w cyberprzestrzeni: jednostki-organizacji-państwa* (Warszawa: CeDeWu).

Challenges for State Security in the Context of Big Data Analysis

JUSTYNA KUREK

Abstract The information society is based on constant access to information. The state also performs its tasks with the use of various information databases and information resources of unstructured nature. These resources include information of personal nature, although, notably, personal data is often only a supplementary element, not constituting the main resource being the focus of attention of the state. New tools, such as big data analysis tools, generate additional obligations in the sphere of information security and protection. The author of this paper makes an attempt to identify the potential threats and problems related to the use of big data tools for the processing of information resources of the state, notably, in the context of "incidental" processing of personal data using big data methods. The objective is primarily to draw attention to the specific risks posed by the loss of control over data by the state and the related security implications.

Keywords: • big data • state security • public registers

CORRESPONDENCE ADDRESS: Justyna Kurek, Ph.D., War Studies University, Faculty of National Security, Department of Political Security, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: j.kurek@akademia.mil.pl, ORCID: 0000-0002-8754-5243.

https://doi.org/10.4335/2022.1.6 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Today's information society is built upon having constant, secure access to the information that is necessary both in professional and private life (Yukins, 2004:668). Beyond the search for information, the ability to cope with its overflow and the need to select useful connections becomes a challenge (Vertinsky, Rice, 2002). The state performs its tasks with the use of various information databases and information resources of unstructured nature. These resources contain information of personal nature, although, notably, personal data is often only a supplementary element, not constituting the main resource being the focus of attention of the state. This situation is well illustrated by the examples found within certain national registers run by Polish authorities, e.g. the Register of Entrepreneurs of the National Court Register and the register gathering information about real properties – the centralised Land and Mortgage Register. There is also a noticeable trend in the evolution of the information resources being managed by public institutions towards broadening them by tapping into unstructured resources, which, more and more often, are created through Internet communication. These resources contain personal data processed by the state and its authorities that are often of sensitive nature.

Under these conditions, which are necessitated by *de facto* continuous data analysis, information management mechanisms and technologies, including big data analysis, are of particular importance. These new tools provide effective support in the implementation of tasks in the area of state and national security, generating, however, additional obligations in the sphere of security and protection of information (Kurek, 2021: 122).

The author of this paper makes an attempt to identify the potential threats and problems related to the use of big data tools for the processing of the information resources of the state, in particular, in the context of "incidental" processing of personal data using big data methods. The assumption is primarily to draw attention to the specific risks posed by the loss of control over data by the state and the related security implications.

2 Big data phenomenon and big data analysis methods

The big data phenomenon is often described as the adoption of new technologies or the application of a set of new technical tools that facilitate data collection and mathematical analysis using traditional statistical methods, as well as more innovative analytical approaches. However, the source literature notes that this view may not fully capture the nature of the phenomenon, especially its power and uniqueness (Mayer-Schönberger, Padovao, 2016: 318). Big data opens up a new perspective on reality. V. Mayer-Schönberger and K. Cukier figuratively define big data processes as "enabling data to speak" (Mayer-Schönberger, Cukier, 2014: 9), while I.S. Rubinstein perceives the big data phenomenon in terms of "steroidally" stimulated data mining processes (Rubinstein, 2013: 76). There is no consensus among legal commentators on the definition and key characteristics of this phenomenon. Certainly, it should be evaluated dynamically

because technological development and new applications significantly affect its understanding and distinguish it from other forms of data analysis (Broeders, Schrijvers, Sloot, Brakel, Hoog, Hirsch, 2017: 310).

It is common to draw attention to three defining qualities figuratively referred to by English language legal commentators as the 3Vs – Volume, Variety and Velocity (Klous, Sustainable, 2016: 27-47). Big data volumes are thus characterised by three basic qualities. The first one is mass availability of data – collected not only from online sources, but also through mobile devices equipped with localisation services and numerous data distribution applications, as well as information from objects equipped with artificial intelligence (Internet of Things) (Hildebrandt 2012: 45-46). The second quality is the use of high speed processing devices and data transfer to achieve cheap and efficient data processing. This analysis more and more often additionally uses the cloud computing model. The third quality is the use of new computing frameworks to collect and analyse massive volumes of data (Rubinstein: 2013: 74). This model can be further complemented by a fourth V (Value) referring to data value (Szafranski, 2015: 11).

Big data processes have undoubtedly changed the face of data analysis, certainly representing a new model of information management in both business and organisational aspects. Indeed, data can be reused for purposes other than the purpose of its original collection. Moreover, data value can be increased not only through new collection and analysis processes, but also by linking data with data from other sources (Kurek, 2021: 126). Data mining also facilitates discovery or inference of previously unknown facts and patterns from the database.

While in the traditional view, data value was manifested in its collection and single use for a specific purpose, big data processes have introduced a revolution, according to which the informational value of data is unclear at the time of their collection (Mayer-Schönberger, Padovao, 2016: 319).

3 Databases in the service of state security

The state and its authorities are the keepers of numerous databases, and most public registers are kept in this form. As M. Kiedrowicz noted in his research, in 2015, according to various sources, the number of registers and records kept in Poland, ranged from 600 to 3000. The scope of information that is collected, stored, processed and further made available by them is vast (Kiedrowicz, 2015: 30). However, this is mostly structured data. It is noted, however, that only 15% of all information produced by humanity is structured and suitable for processing using relational database methods and tools. The remaining 85% constitutes a large 'reservoir of data', whose informational content is undoubtedly invaluable, but due to its unstructured nature, is unsuitable for processing in an organised manner (Dygaszewicz, 2015: 49). Its re-analysis and use by public authorities is only possible due to the potential of big data technology, which facilitates re-organisation and

re-analysis of resources for the purpose of obtaining information, the potential of which was not originally envisaged.

The use of big data analysis for the performance of the tasks in the area of state and national security is a major challenge currently faced by state authorities. These challenges are of both organisational and legal nature. Having regard to the principle of legalism, the state authorities may act only within and under the law, therefore, without an appropriate legal basis; they may not process data for purposes other than those for which they were collected. Moreover, the very process of data collection requires an adequate legal basis. Taking into account the fact that in the case of big data processes, the purpose of data use is *de facto* not known at the moment the data comes into possession, the processing of big data may pose particular challenges for public authorities (Kurek, 2021: 138).

It is, therefore, difficult to organise the protection of information in a preventive manner if the way it will be used and linked to other data is not fully known. A key element of data and information management policy at the initial stage of the legislator's decision to create a relevant resource and database (in particular, one that contains personal information) should be proper risk analysis. Such analysis should include both an in-depth reflection on the processes connected with processing, safety of collection and sharing of data, but also on the security of data sets, so that in case of losing control over given data, it cannot be easily used or manipulated.

Structured data aggregated into a relational database pose a huge challenge in the sphere of security. It is insufficient from the security point of view to concentrate only on the external layer and on securing only entry to the system. Breaching the external security protecting against all forms of unauthorised access may be just a matter of proper combination of queries to the database and de facto be a security bypass, not a security breach. A perfect example is the bypass of security protecting the land and mortgage register resource, which took place several years ago. The only real security of this system protecting against an automatic takeover of the resource by means of automatic queries is the CAPTCHA mechanism, which *de facto* does not generate protection against automated access (Ahn, Blum, Langfords, 2004: 57-60).

4 The *casus* of re-use of land and mortgage register data

The risks for state security and privacy are perfectly illustrated by the example of re-use of the data in the Land and Mortgage Register. An entity having its registered office in the Seychelles collected and indexed information from over twenty million land and mortgage registers (Gryszczyńska, 2017: 298). This procedure was possible even though, theoretically, public access to land and mortgage registers is possible only through one search criterion – the land and mortgage register number. The collection of the specified resource was not the outcome of obtaining the unique numbers of over twenty million land and mortgage registers, nor of breaking the security measures and obtaining data in

an illegal manner. The entity that collected the specified information did so by working out how the land and mortgage register numbers were constructed.

It should be noted that the register number consists of three predefined elements: a court district code (to be selected from a list), a specific number consisting solely of digits and a checksum between 0 and 9. Taking into account the limited number of specific numbers and knowledge of the two additional elements of the register number, created for the purpose of database queries and obtaining information, a list of potential numbers of land and mortgage registers was easy to generate. It was therefore relatively easy to extract the structured data and re-enter it into databases managed by another entity and to apply additional search criteria (e.g. real property address, plot registration number, owner's name, existence or not of mortgage encumbrances). This way, through the re-use of public information, it was possible to build a system facilitating extraction of information about owners of specific real properties or to simply obtain information about mortgage encumbrances and the amount of loans with which a given real property has been financed. This information could be easily used for criminal purposes and might be an excellent source of information for criminals, as noted in available studies on this subject (https://www.rp.pl/artykul/988227-Ksiegi-wieczyste--wyciekly-dane-o--16-milionach-hipotek-w-Polsce.html).

This generates not only the risk for the privacy and security of specific individuals, but also for the state and its authorities, which, as one of their key objectives, ensure security to its citizens, as well as all persons and property on their territory. Land and mortgage registers contain information on the property and possessions of key people in the state. The address data provided in the system also facilitate a potential identification of the place of residence of the key persons in the state.

Extracting the information in question was not the outcome of a criminal offence or a breach of security, nor was it the outcome of unlawful entry into possession of state-managed information. It was the outcome of security bypass and re-use of public information in accordance with the law in force. The structuring of the data only facilitated the reprocessing. One could wonder whether in this situation it is possible to speak of an abuse of right in the meaning of Article 5 of the Civil Code, i.e. the use of a subjective right (the right to re-use public information) contrary to its socio-economic purpose or principles of community life. In my opinion, such interpretation is too far-reaching and *de facto* annihilates the political objective of the institution of re-use of public information.

Of course, the question should be asked whether meeting the objective of openness of land and mortgage registers required such a form of access to data and their full centralisation, as it was done by the Polish legislator, who decided to fully digitalise and centralise public registers. It is worth mentioning the examples from, for instance, Germany, where obtaining an extract from the land and mortgage register is done through the portal of justice (www.justiz-portal.de). In Germany, data sets were not centralised

and there is not just one database. The website, referred to above, only contains links to the portals maintained in individual states (Länder). Access groups and gradation of access rights have also been introduced. For example, unconditional and full access is granted to notaries and real estate institutions (insurers, banking institutions, administrative offices, courts). For others, access is possible but only upon fulfilment of access conditions and, in some cases, upon payment of a symbolic fee.

Perhaps in Poland we should also think of decentralisation of registered data sets, by way of consolidation of the same through common links. It is also worth considering whether the information should not be managed in the form of a database system or if it would be sufficient to make it available in a form aggregated to a closed pdf format with protection against copying. One could also set a question if, from a security point of view, the procedure for numbering of the register should not be re-established, so that they are numbered at random rather than according to a template. Perhaps the difficulty of working with such a system and managing such data would not outweigh the gain in information security.

It is also worth asking if at least some of the personal data included in the public resource should not be anonymised or hidden. From the point of view of security of the conduct of legal transactions, information that is truly important is the mortgage collateral, but the information about the value of the collateral could be available only to entities having legal interest in obtaining such information. Indeed, from the point of view of state security, security measures and access levels may play two functions: on the one hand, they facilitate the control of information managed by the state, on the other hand, they introduce the control of access and make it possible to record the recipients of information.

Public access to data in the land and mortgage register also implies the use, in the conduct of legal transactions (with the legislator's consent), of extracts from the register made individually in an unauthorised manner. The practice is that extracts from the register are made personally by the parties to a legal transaction and attached to the documentation. When unauthorised sets of information are created using reprocessed public information, there is also a risk that extracts from such private databases will be made and submitted instead of extracts from public registers. In the case of such private database systems, the consolidation of information and its accuracy is not covered by the public quality guarantee in the form of, in the case at hand, the warranty of public credibility of land registers.

5 Conclusion

As perfectly illustrated by the example of the processing of land and mortgage register data in the Seychelles, unauthorised re-use of personal data by a data controller reveals a completely new potential of data abuse. This often implies a serious security risk for persons whose data is – even incidentally – processed. Therefore, one should ask if the

potential of using big data tools outweighs the threats and challenges for state security posed by consolidation and integration of data of various provenance in terms of big data. In practice, loss of control over data and security threats do not necessarily result from illegal access to information. They are often the result of lawful use of public information in the mode of re-use of public information for a purpose other than the purpose of its extraction. Hence, when it comes to information management, particularly in the era of big data analysis, risk analysis is crucial. This applies across the board to those processes where the data potential is unknown to the data controller at the outset. Effective information security management requires preventive measures, and, just as in war, the greatest success is to defeat the enemy without a fight, so in the case of information security the most important issue is to effectively predict and counteract the risks. The revealed loopholes in the system, which result from legal regulations, on the one hand, and from the possibility to implement them, on the other hand, indicate that the lack of risk analysis and adequate data and information processing security may result in the risk of losing control over data exceeding the advantages related to the potential of big data and data consolidation from various resources.

References:

Ahn, L., Blum, M. & Langfords, J. (2004) Telling Humans and Computers Apart Automatically, *Communications of the ACM*, 47(2), pp. 56-60.

Broeders, D., Schrijvers, E., Sloot, B., Brakel, R., Hoog, J. & Hirsch, E. (2017) Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data, *Computer Law & Security Review*, 33(3), pp. 308-323.

Dygaszewicz, J. (2015) Big data w statystyce publicznej, In: Szpor, G. (ed.) *Internet. Publiczne bazy danych i Big Data* (Warszawa: C.H.Beck), pp. 49-63.

Gryszczyńska, A. (2017) Nowe zagrożenia rejestru ksiąg wieczystych, In: Szpor, G. & Gryszczyńska, A. (eds.) *Internet. Strategie bezpieczeństwa* (Warsaw: C.H.Beck), pp. 293-310.

Hildebrandt, M. (2012) The Dawn of a Critical Transparency Right for the Profiling Era, In: Bus, J., Crompton, M., Hildebrandt, M. & Metakides, G. (eds.) *Digital Enlightenment Yearbook* (Amsterdam: IOS Press), pp. 41-56.

Kiedrowicz, M. (2015) Dostęp do publicznych zasobów danych. Big data czy big brother, In: Szpor, G. (ed.) *Internet. Publiczne bazy danych i Big Data* (Warszawa: C.H.Beck), pp. 15-41.

Kurek, J. (2021) *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big data. Aspekty prawne, organizacyjne i systemowe* (Warszawa: ASzWoj).

Mayer-Schönberger, V. & Cukier, K. (2014) *Learning with big data* (Boston-NewYork: Houghton Mifflin Harcourt Publishing Company).

Mayer-Schönberger, V. & Padovao, Y. (2016) Regime Change? Enabling Big Data through Europe's New Data Protection Regulation, *The Columbia Science and Technology Law Review*, 17(2), pp. 317-334.

Rubinstein, I.S. (2013) Big Data: The End of Privacy or a New Beginning?, *International Data Privacy Law*, 3(2), pp. 74-87.

Szafrański, B. (2015) Realizacja zadań publicznych a Big data, In: Szpor, G. (ed.) *Internet. Public databases and Big Data* (Warszawa: C.H.Beck), pp. 3-15.

Vertinsky, L. & Rice, T.M.. (2002) Thinking about Thinking Machines: Implications of Machine Inventors for Patent Law, *Boston University Journal of Science and Technology Law*, 2, pp. 574-613.

Yukins, C.R. (2004) Making Federal Information Technology Accessible: A Case Study in Social Policy and Procurement, *Public Contract Law Journal*, 33(4), pp. 667-725.

The Competence of the Internal Security Agency in Protecting the Security of Communication and Information Systems and Networks of Public Administration Authorities

MIROSŁAW KARPIUK

Abstract The Internal Security Agency (ISA), which is one of Poland's special services, has competence over matters entailing the protection of the state's internal security and its constitutional order. Its tasks include the identification, prevention and combating of threats to the internal security of the state and its constitutional order, in particular those affecting the sovereignty and international status of the state, its independence and inviolability of state borders, as well as the state defence capabilities. The ISA is also obligated to protect the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or the system of ICT networks which are included in the uniform list of facilities, installations, devices and services which comprise critical infrastructure. Cyberspace is one of the areas of operations pursued by this civil intelligence service, where its task is to protect communication and information systems of primary significance to the functioning of public administration within the framework of state structures.

Keywords: • special services • cybersecurity • communication and information systems • ICT networks • public administration

CORRESPONDENCE ADDRESS: Mirosław Karpiuk, PhD., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ul. Obitza 1, 10-725 Olsztyn, Poland, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

https://doi.org/10.4335/2022.1.7 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Communication and information systems and networks are exposed to cyber-attacks, so the telecommunications infrastructure should be continuously protected in order to prevent such threats. The Internal Security Agency (ISA) has the obligation to provide such protection. The competence of the ISA in respect of identifying, preventing and combating threats to the security of communication and information systems of public administration authorities is falls within the domain of cybersecurity. The tasks of this special service include the provision of security in cyberspace. Cyberspace is understood as a space for the processing and exchange of information, comprised of communication and information systems, including the links between them and their relations with users (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 1).

The challenges posed by the new digital era have compelled public administration authorities to introduce changes (Hoffman, Cseh, 2020: 210). Contemporary public administration acts on the basis of communication and information systems and networks that need to be properly protected against cyber-attacks. The role of the state is to ensure cybersecurity within public institutions. The National Cybersecurity System Act of 5 July 2018 (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended), as per Article 2(4), defines cybersecurity as the resilience of information systems against operations that compromise the availability, authenticity, integrity and confidentiality of processed data, or the related services offered by those information systems. Cybersecurity constitutes a specialised security system component that covers the protection of information systems against threats (Czuryk, 2019: 42).

2 The competence of the Internal Security Agency in cybersecurity

The Internal Security Agency (ISA) is a civil special service which has, like other special forces, competence over security affairs (Bożek, Czuryk, Karpiuk, Kostrubiec, 2014: 43). It was established to protect the internal security of the state and its constitutional order. This competence arises from the provisions of Article 1 of the Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency (consolidated text, Polish Journal of Laws of 2020, item 27, as amended) – further referred to as "the AISA". This general competence of the ISA also encompasses the provision of cybersecurity in public administration through the protection of communication and information systems and networks operated by public administration. The statutory responsibilities of the ISA include the identification, prevention and investigation of threats to the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or ICT networks that are included in the uniform list of facilities, installations, devices and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners or holders of critical infrastructure facilities, installations and devices, as

expressly laid down in Article 5(1)(2a) of the AISA. In line with the definition set out in Article 2(3) of the Act of 18 July 2002 on the Provision of Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344, as amended), a communication and information system is a set of cooperating IT hardware and software providing the capability to process and store, as well as send and receive, data via ICT networks with the use of telecommunications terminal equipment suitable for a given network type. Under Article 2(43) of the Telecommunications Law of 16 July 2004 (consolidated text, Polish Journal of Laws of 2021, item 576, as amended) telecommunications terminal equipment is understood as telecommunications devices intended for direct or indirect connection with network termination points. An ICT network includes software operated by the devices that have access to it, allowing users to browse, create, disseminate and exchange data and information (digital content) as part of network access (Chałubińska-Jentkiewicz, 2019: 132). Critical infrastructure is understood as systems and functionally linked facilities forming part of the systems, including buildings, devices, installations, essential services of key importance to the security of the state and its citizens, and services intended to provide efficient operations of public administration authorities, institutions and enterprises - Article 3(2) of the Crisis Management Act of 26 April 2007 (consolidated text, Polish Journal of Laws of 2020, item 1856, as amended), hereinafter "the CMA".

3 The assessment of the security of communication and information systems of public administration authorities that are significant for the continuity of state functioning

Due to the need to ensure cybersecurity in public administration, as per Article 32a(1) of the AISA, the ISA is obliged to assess the security of communication and information systems and networks. This is undertaken with a view to preventing, counteracting and combating terrorist incidents that may affect the communication and information systems of public administration authorities that are significant for the continuity of state functioning, and/or ICT networks which are included in the uniform list of facilities, installations, devices, and services that comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems. The ISA is also compelled to prevent and investigate terrorist offences affecting this sphere, and to prosecute the perpetrators of such offences. To these ends, the ISA may assess the security of these communication and information systems. This last is not an obligation on the part of this special service, but a power that it should, nonetheless, exercise where a terrorist threat occurs. As stipulated in Article 5b(7)(1) of the CMA, the Head of the Government Centre for Security, in collaboration with competent ministers, prepares a uniform list of facilities, installations, devices and services which comprise critical infrastructure, divided by systems, and classified. It also includes European critical infrastructure located on the territory of the Republic of

Poland, and European critical infrastructure located on the territories of other EU Member States that might have a significant impact on Poland. The list is classified.

The objectives of the assessment of communication and information systems of public administration authorities are to prevent, counteract and combat terrorist incidents, and to prevent and investigate terrorist offences affecting this sphere, and prosecute their perpetrators. Under Article 2(7) of the Act of 10 June 2016 on Counter-Terrorism Measures (consolidated text, Polish Journal of Laws of 2019, item 796, as amended) a terrorist incident is understood as a situation where there is a suspicion that such incident has occurred as a result of a terrorist offence, or where a threat of such offence has been identified. In turn, a terrorist offence is a prohibited act subject to imprisonment with the upper sentence limit of at least 5 years, committed with the aim of seriously intimidating a population, unduly compelling a public authority of the Republic of Poland or another state Government or international organisation to perform or abstain from performing an act, or seriously destabilising or destroying the structures or the economy of the Republic of Poland, another state or an international organisation, or a threat of committing such act, as stipulated in Article 115 § 20 of the Act of 6 June 1997 – the Penal Code (consolidated text, Polish Journal of Laws of 2020, item 1444, as amended), hereinafter "the PC".

Pursuant to Article 32a(2) of the AISA, the assessment of the security of communication information systems and networks is performed in line with the annual security assessment plan, prepared by 30 September in the preceding year by the Head of ISA, in consultation with the minister in charge of computerisation. Where justifiable, the security assessment may be performed even if it has not been included in the plan. Planning, including with regard to cyberspace, facilitates coordinated measures allowing a proper, timely and balanced performance of tasks assigned to public administration in a well-organised and uninterrupted manner (Karpiuk, 2021: 46). As a rule, the annual plan is the basis for performing the assessment of the security of communication and information systems. The plan is the outcome of cooperation between the Head of ISA (as a central government administration body) and the minister in charge of computerisation (responsible for managing an administration department which entails matters related to communication and information systems and networks of public administration). The cooperation assumes a specific form, i.e., consultation.

The ISA informs the entity managing a given communication and information system that the system is to be included in the annual security assessment plan. This information obligation is imposed under Article 32a(3) of the AISA. The information concerning the date and range of security tests to be performed allows a proper preparation for assessment, including certain restrictions on the performance of public tasks by the administration body whose communication and information system is to be tested.

As per § 4(1) of the Regulation of the Council of Ministers of 19 July 2016 on the performance of security assessment in relation to preventing terrorist incidents (Polish Journal of Laws of 2016, item 1076), hereinafter "the SAR", prior to security assessment, the ISA requests the entity which manages the system concerned to provide information about the system, which may include: 1) system architecture (system architecture is a description of the components of a communication and information system or an ICT network, and their links and relationships to each other), including information on the hardware forming part of the system infrastructure; 2) IP addressing of the system's network infrastructure; 3) information on the current backup copy and the rules of its update, 4) definition of the required system recovery time based on the backup copy; 5) information on the test environment and its range, 6) ICT security features, 7) system security procedures, 8) details of the person appointed by the system managing entity to contact the ISA during the security assessment on an ongoing basis, and 9) details of the person authorised to represent the system managing entity. Given the objective to be achieved by the assessment of the security of communication and information systems of public administration authorities, i.e. counteracting terrorism, the information requested by the ISA should be provided. The information about communication and information systems disclosed to the ISA allow it to perform a full security assessment.

Pursuant to Article 32a(4) of the AISA, security assessment involves security tests on a communication and information system with a view to identifying vulnerabilities, understood as weak points of resources or a security features in a communication and information system which may be used by a threat source and affect the integrity, confidentiality, accountability, and accessibility of the system. Improper security of a communication and information system of a public administration authority might result in its disrupted operations. Cyberthreats can lead to disruptions in the functioning of public institutions, which directly affects their security.

Security assessments are performed in line with the minimisation principle. Pursuant to the provisions of Article 32a(5) of the AISA, the ISA should perform the assessment subject to the principle of minimising the interruptions in system operations, or its restricted availability, and may not result in irreparable damage to data processed in the communication and information system undergoing assessment. In turn, as per Article 32a(6) of the AISA, in order to minimise the adverse effects of security assessments, the ISA consults the framework conditions for conducting such assessment with a relevant public administration authority, in particular, the commencement date, the schedule, as well as the range and type of security tests performed as part of the assessment. The performance of security assessment may not hinder, or significantly restrict the operations of the public administration authority that is obliged to ensure the continued performance of its tasks. Public affairs must be arranged in an uninterrupted manner, and therefore security assessment cannot be a reason for closing a given office (or its individual organisational units), being a subsidiary entity of a public administration body, if it

becomes impossible to use its communication and information system for an extended period of time. Interference with the operations of a communication and information system of a public administration authority cannot be excessive. It should not result in permanent damage to the data processed in the system, which is required for the tasks performed by such authority.

Under Article 32a(7) of the AISA, the legislators provided the ISA with a possibility to develop or acquire computer hardware or software, and use it to determine the vulnerability of the system being assessed to the risk of the commission of an offence which: 1) results in the endangerment to the lives and health of a large population or property of a significant size, by blocking, or otherwise affecting automatic processing, collection or transmission of IT data (Article 165 § 1(4) of the PC; 2) includes the fixture and/or use of an eavesdropping device, visual device or other type of device or software with a view to obtaining unauthorised access to information (Article 237 § 3 of the PC). This provision penalises the interception of computer data during transmission (Radoniewicz, 2019: 203); 3) includes unauthorised destruction, damage, deletion, change and/or obstructed access to IT data, or significant disruption or prevention of the automatic processing, storage and/or transmission of such data - including activities causing significant damage (Article 268a § 1-2 of the PC; 4) includes the destruction, damage, deletion and/or change of IT data of significant importance to the state defence capabilities, security in communication, the functioning of public administration, other state bodies or local government institutions, or the disruption or prevention of the automatic processing, storage and/or transmission of such data – by destroying or replacing a computer storage medium, or by destroying or damaging a device used for the automated processing, storage and/or transmission of IT data (Article 269 § 2 of the PC); 5) includes a significant disruption of the operation of an IT system, a communication and information system and/or an ICT network, through the transmission, destruction, deletion, damage, obstructed access and/or change of IT data, without being authorised to do so (Article 269a of the PC). The analysed provision (Article 32a(7) of the AISA) constitutes a justification (Opaliński, Rogalski, Szustakiewicz, 2017: 150).

The activities performed as part of security assessment are defined in § 3(1) of the SAR and they include: 1) passive data collection – collecting online information related to the functioning of the system with impact on its security, 2) semi-passive data collection – collecting information in the system to identify data related to the functioning of the system with impact on its security, in line with the rules applicable to system users, excluding actions which require authentication in the system. These activities may be supplemented by collecting information arising from system architecture analysis; 3) active data collection – collecting information in the system to identify data related to the functioning of the system with impact on its security, using a method which goes beyond the authorisations of a system user, including actions which require authentication in the system, in particular, actions consisting in the enumeration of services, ports, detection

of intermediate devices, the detection of IDS/IPS and firewalls; 4) the identification of vulnerabilities in system architecture and web services – undertaking measures aimed at identifying vulnerabilities to threats based on the collected information about system architecture, provided by the system managing entity.

The information obtained by the ISA in the course of security assessment constitute confidential information protected by law and as such may not be used for the performance of other statutory tasks entrusted to the ISA, and it is subject to immediate destruction in the presence of a committee which draws up minutes of the said action. This obligation is imposed under Article 32a(9) of the AISA. The Head of ISA orders that the materials be destroyed immediately upon the completion of security assessment. He/she appoints three committee members taking part in the destruction of materials. The committee is composed only of officers who are members of the ISA organisational unit that performs the security assessment. The materials must be destroyed through: 1) permanent removal of information recorded on computer storage media or their copies on which the information has been saved, in a way which makes it impossible to recover the contents of the recorded data; 2) physical destruction of materials and documents drawn up on their basis, with the use of a shredding device, in a way which makes it impossible to read the contents. The above rules are stipulated in §§ 2 and 3 of the Regulation of the Prime Minister of 18 July 2016 on the methods of destroying materials containing information obtained in the course of security assessment performed by the Internal Security Agency, and on the templates of the required documentation (Polish Journal of Laws of 2016, Item 1055).

If it is found that a terrorist incident has occurred in respect of communication and information systems of public administration authorities that are significant for the continuity of state functioning, The Head of ISA, under Article 32b(1) of the AISA, may request the system managing entity to provide information about the design, functioning, and operating principles of the communication and information systems in their possession, including information on computer passwords, access codes and other data enabling access to the system and its use, with a view to preventing and responding to terrorist incidents affecting such systems, and to preventing and investigating terrorist offences in this sphere, and prosecuting their perpetrators. The information is required for the ISA's performance of its statutory tasks. Pursuant to Article 32b(1) of the AISA, the information is subject to protection as stipulated in the provisions governing the protection of classified information, and may only be disclosed to ISA officers who run investigative operations as part of the given proceedings, and to their superiors who are authorised to supervise the said activities. As per Article 1(1) of the Act of 5 August 2010 on the protection of classified information (consolidated text, Polish Journal of Laws of 2019, item 742, as amended), classified information means those pieces of information whose unauthorised disclosure would or potentially might result in damage suffered by

the Republic of Poland, or would be detrimental to its interests, also in the course of the development of such information, notwithstanding its form and means of expression.

4 An early warning system for threats on the Internet

With a view to preventing, counteracting and combating terrorist incidents which affect communication and information systems of public administration authorities that are significant for the continuity of state functioning and/or ICT networks which are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems, as well as to prevent and investigate terrorist offences affecting this sphere, and to prosecute the perpetrators of such offences, under Article 32aa (1) of the AISA, the ISA is obliged to implement in the said entities an early warning system for threats on the Internet, as well as to manage and coordinate its operations. The implementation of an early warning system for threats on the Internet is aimed at combating terrorism. Given the above, public administration authorities are obliged to join the early warning system and provide the ISA with required information allowing the implementation of the early warning system in these entities. This obligation is imposed under Article 32aa(4) of the AISA.

As a rule, the early warning system within the infrastructure of a given public administration authority is implemented on the basis of the annual plan. As stipulated in § 2 of the Regulation of the Prime Minister of 2 January 2020 on the conditions and procedure for managing, coordinating and implementing an early warning system for threats on the Internet (Polish Journal of Laws of 2020, item 54), hereinafter "the REWS", the ISA provides a public administration authority where the early warning system is to be implemented in line with the annual implementation plan with information about: 1) the technical aspects of participating in the early warning systems, which are required for its implementation, in particular, start up; 2) the proposed time limit for the implementation of the early warning system.

By way of an understanding, the ISA consults and agrees upon, with a given public administration authority, the technical aspects of participating in the early warning system and the system configuration model. The ISA does not impose its vision of this body's participation in the early warning system, but enters into negotiations with a view to establishing a common position in this respect. Nonetheless, where it is impossible to reach an understanding for reasons attributable to the public administration authority, pursuant to Article 32aa (8) of the AISA, the ISA must notify a supervisory authority or the minister in charge of computerisation.

Participation in the early warning system is subject to the fulfilment of obligations arising from § 5(1) of the REWS, namely: 1) the obligation to immediately remove any malfunctions of network infrastructure powering the early warning system, to maintain its full working order; 2) to monitor and analyse, using own resources, the information generated by the early warning system in order to undertake remedial and safeguarding measures covering the said system; 3) to refrain from providing information to other entities: a) information about the early warning system, b) the whole or part of the software and hardware platform provided by the ISA, c) information about the hardware platform forming part of the early warning system, and about the technical aspects related to the design and operation of the system.

5 Conclusions

Counteracting threats in the cyberspace, including cyberterrorism, will be possible if a high level of security is maintained in communication and information systems of public administration authorities which are significant for the continuity of state functioning and/or ICT networks that are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure, as well as the communication and information systems belonging to the owners, owner-like possessors or lessees of critical infrastructure facilities, installations and devices, or of the data processed in the said systems.

In Article 32e of the AISA, the legislators have introduced the recommendation institution, whose aim is to increase the level of security of communication and information systems. The Head of ISA carries out the analysis of incidents that compromise the security of communication and information systems, and issues recommendations to public administration authorities in order to increase the level of security of communication and information systems with a view to ensuring their integrity, confidentiality, accountability and accessibility. The public administration body concerned may submit its reservations to the recommended methods for increasing the level of security of its communication and information systems due to the adverse effects of the recommended measures on the functionality of the system or the occurrence of new vulnerabilities, though no later than within 7 days of the date it receives the recommendations. The Head of ISA expresses his/her position on the reservations, and upholds the recommendations in question, or provides amended recommendations. The body that has received the recommendations must notify the Head of ISA on the method and range of their implementation within a month of their receipt. The failure to implement the recommendations constitutes grounds for the Head of ISA to notify the authority supervising the operations of the public administration authority concerned that the recommendations are not taken into account, or to request that action be taken to implement the recommendations.

References:

Bożek, M., Czuryk, M., Karpiuk, M. & Kostrubiec, J. (2014) *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe* (Warszawa: LEX a Wolters Kluwer business).

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: Lex Localis), 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.

Hoffman, I. & Cseh, K. (2020) E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary, *Cybersecurity and Law*, 2, pp. 199-211.

Karpiuk, M. (2021) Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 1, pp. 45-52.

Opaliński, B., Rogalski, M. & Szustakiewicz, P. (2017) *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz* (Warszawa: C.H.Beck).

Radoniewicz, F. (2019) Przestępstwa komputerowe w polskim Kodeksie karnym, *Cybersecurity and Law*, 1, pp. 193-212.

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

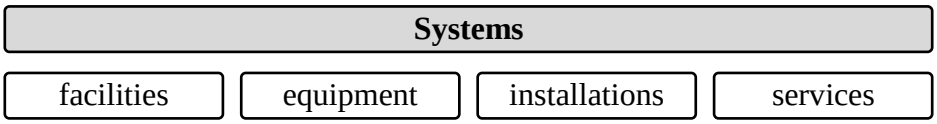
Critical infrastructure – which provides fundamental services such as the supply of energy, energy resources and fuels, communications, ICT networks, food and water – plays a key role in the functioning of a modern state. Hence, one of the primary tasks of the state is to ensure adequate protection, 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).

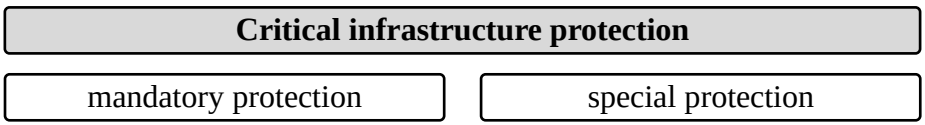
Security always applies to various manifestations of human activity. The basic attributes of security that apply to communication processes include confidentiality, which means that only authorised persons have access to certain data and information. The second element is integrity of digital content,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

LEX LOCALIS

The Use of Cybersecurity-specific Research Methods to Identify Behaviours Preceding Dangerous Traffic Situations

KAZIMIERZ PAWELEC

Abstract Traffic disasters, situations creating the danger of a disaster and road accidents are usually preceded by dangerous activities of individuals who, by act, negligence, or non-compliance, bring about hazardous situations. Such behaviours can be caused by a range of factors, including those that are specific to humans, who are considered to be the weakest link in the entire system of road traffic safety. Hazardous situations can also result from public servant passivity, the lack of reaction to recorded behaviours, defective roads, inappropriate traffic markings, signage and organisation, and from allowing dangerous vehicles on the road. In this article, the author makes an attempt at identifying participant-induced dangerous behaviours. Based on an analysis of traffic camera material, he proposes to develop an algorithm to recognize individuals whose risky behaviour may induce traffic mishaps, hence, allowing prompt measures to be put in place to prevent them from creating dangerous road situations. Furthermore, the paper argues that uniform driving fitness requirements should be imposed across the European Union. It also draws attention to the existing shortcomings in knowledge about the aetiology of traffic crimes, and to the misguided focus of EU Member States' authorities on repressive measures – which fail to deliver the expected outcome of improved road traffic safety.

Keywords: • traffic crimes and petty traffic offences • intoxication • dangerous behaviours • preventive measures

CORRESPONDENCE ADDRESS: Kazimierz Pawelec, Ph.D., Assistant Professor, Siedlce University of Natural Sciences and Humanities, Faculty of Social Sciences, Institute of Security Science, S. Konarskiego 2, 08-110 Siedlce, Poland, e-mail: pawelec.kancelaria@op.pl, ORCID: 0000-0001-8669-0249.

https://doi.org/10.4335/2022.1.9 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Impaired psychomotor reactions of the driver can clearly lead to traffic disasters, the immediate danger of a disaster, or a traffic accident. Many factors can play a role in weakening psychomotor abilities, including those attributable to the driver, i.e. intoxication with alcohol or other psychoactive substances, tiredness, poor health and personality-related factors. This publication has significance for traffic safety, as it attempts to identify, and possibly eliminate, so-called hazardous drivers before they can create specific dangerous situations. Accordingly, the research aim was to develop methods of identifying such individuals before they can take risky, hazardous actions or commit omission. This required devising an internal safety system using cybersecurity-specific methods in order to, in a way, pre-emptively eliminate such individuals from traffic by taking purely preventive measures and developing legal regulations underlying these measures such that they are accepted by the general public without the need to use more repressive methods. This has become more important in that the deterring approach has clearly proven to be ineffective.

One more important issue to consider – highly relevant although beyond the scope of this paper – is related to the significant technological advancements, especially in IT. Indeed, many cars, especially premium class vehicles, are equipped with a range of driving assistance devices, and in some countries, such as China, Canada and the US, so-called "autonomous vehicles" are allowed on the road, where human involvement in driving the car does not go beyond stating the destination. Consideration, therefore, should be given to the possibility of unauthorised intrusion into the IT system of the vehicle to disrupt its operation and cause an accident or disaster. The question, therefore, arises – would it be possible to identify such intrusion before the disruption occurs, and what signs could precede such disruption? In short, we should consider what could serve as research material. Surprisingly, such material already exists and has been successfully used for more than ten years. It is the data recorded by traffic cameras that are now commonly used in many cities and on highways. The employment of such material should not be considered as contributing to repressiveness. Rather, it should be considered as being research material that is useful in developing an algorithm that could help to identify and correctly interpret reactions and other external signs preceding behaviours that are dangerous to others. This is also one of the research aims of this publication. However, these considerations also require at least a synthetic examination of the legal solutions related to the typification of traffic crimes and petty traffic offences, as exemplified by the Republic of Poland. Another important step is to discuss the factors behind traffic hazards caused by traffic participants, and subsequently to name the contributing factors and behaviours relevant to the identification of a future hazard. In conclusive remarks, the author proposes, among others, legislative solutions, including those relating to the EU law, as well as *de lege lata*, that are important for practical considerations, such that the focus is not only on the consequences, but also on the causes, shifting towards preventive measures, and moving away from repression – treating this as a last resort.

2 The typification of traffic crimes and petty traffic offences in Polish law – basic facts

Crimes against traffic safety are listed in Chapter XXI of the Penal Code of 6 June of 1997 (uniform text, Polish Journal of Laws 2020, item 1444, as amended) (further referred to as "the PC"). The legislators have listed eight misdemeanours against the above-mentioned legally protected right, with only three of them bearing specific consequences, i.e. a disaster (Article 173 PC), creating the immediate danger of a disaster (Article 174 PC), and an accident (Article 177 PC). It should be noted that the above-mentioned misdemeanours are common, with only one of them – accident – considering the violation, including unintentional violation, of safety rules in land, water or air traffic as being an objective element of the prohibited conduct. This does not necessarily mean that the occurrence of a disaster, or the creation of the immediate danger of a disaster, cannot relate to these rules. However, only an accident can be caused inadvertently, whereas a disaster, or the immediate danger of a disaster, can be caused by wilful misconduct through both direct and oblique intent. The legislators have introduced harsher penalties for perpetrators of acts set out in Articles 173, 174, and 177 of the PC, who were intoxicated by alcohol, under the influence of a psychoactive substance, or who fled the scene. They have restricted punishability to drivers of motor vehicles who were driving when intoxicated by alcohol or under the influence of a psychoactive substance (Article 178a PC), or who attempted to escape a chase taken up by a traffic officer (Article 178b PC). Another crime that may be perpetrated only by individuals operating motor vehicles involves driving a motor vehicle despite a revoked driving license (Article 180a PC).

Other provisions of Chapter XXI of the PC provide for the criminal liability of, for instance, a dispatcher who allows the operation of a motor vehicle, or other vehicle, in a condition which directly endangers the safety of land, water or air traffic despite being under a specific obligation to the contrary, or of an individual who is performing traffic safety duties when intoxicated by alcohol or under the influence of a psychoactive substance (Article 180 PC). Of course, the liability of such individuals referred to in Articles 179 and 180 of the PC is not excluded in the event of their causing a disaster, the immediate danger of a disaster or an accident in line with the concept of extended liability, provided that this is warranted by evidence (Pawelec, 2020: 297-302).

Petty offences against road traffic safety and order are typified in Chapter XI of the Code of Petty Offences of 20 May 1971 (uniform text, Polish Journal of Laws 2021, item 281, as amended) (further referred to as "the CPO"). The main idea behind this law was to provide a full catalogue of petty offences against road traffic safety, and to facilitate the application of a "range of laws", such that petty offences deserving harsh treatment were not treated lightly and, conversely, that the application of such laws would not be overused through the formalistic interpretation of Chapter XI provisions of the PC

(Bardach, 1980: 441). Over the years, however, practical experiences revealed that these provisions were deficient. This was particularly true for the vague provisions that provided general descriptions of prohibited acts or contained references to other regulations. Judged on their merits in terms of ensuring road traffic safety and order, they also had repeatedly proven questionable. The prevailing approach was formalistic, specific to administrative authorities, and as such having little to do with the dynamics, variability and atypicality of road traffic situations (for instance – failure to follow signs, signals or instructions in road traffic – Article 92 CPO; using a vehicle registration certificate that contains false information – Article 95a CPO). The same formalistic approach was adopted in respect of perpetrators of petty offences against traffic order (for instance – failure to clean the road despite being under the obligation to do so –Article 101 CPO; failure to keep access points in a proper condition – Article 102 CPO).

Judging by the system of petty offences in Chapter XI of the PC, it is evident that the prime importance in terms of ensuring safety and eliminating dangers was attached to those petty offences that posed a direct threat to road traffic safety. However, in practice, as well as in interpretations by legal commentators, there was one important aspect that could not be ignored – namely, the repeated atypicality of traffic situations. Legal regulations, including in particular the Traffic Law Act of 20 June 1997 (uniform text, Polish Journal of Laws of 2021, item 450, as amended), which was extensively referred to in the Code of Petty Offences, as were the general safety rules, assume the existence of a certain model of typical behaviours in typical situations. Once this typicality is disrupted, however, it becomes necessary to bring a response that deviates from this model. Traffic participants not only have the right, but also the obligation, to eliminate or minimise dangers on the road. Typical petty offences against road traffic safety are ones that carry a potential for danger to others, as well as to the perpetrator. The danger had to be real. This is the consequence referred to in Article 86 CPO – creating a danger to traffic safety; Article 93 CPO – failure to help a victim of an accident; Article 97 CPO – violating provisions on road traffic safety and order; Article 98 CPO – failure to exercise caution when driving on internal roads, as well as Article 87 CPO – driving after the consumption of alcohol or other substance with similar effects.

3 The weakest link – is it only man?

Overall, when considering issues around traffic crimes and petty traffic offences, as briefly described above, it should be emphasised that state authorities pass legislation that essentially shifts responsibility to humans – the weakest link of the entire system, one could say (Pawelec, 2021: 27-161). The commonly accepted approach is one of attributing guilt for all road traffic accidents to people. This is the approach that guides all criminal and petty-offence procedures. Yet, state authorities fail to fulfil their obligations and refuse to accept responsibility for their officers – and are absolutely unwilling to admit this. They consider human mistakes – made by traffic participants – as the primary, if not the only, cause of any road incident, forgetting that it is them that

bear responsibility for the condition of roads and associated equipment, traffic organisation and the elimination of identified threats (Pawelec, 2017: 13-14). What they do is engage in the art of manipulation by using a variety of methods, including: "blame attribution", "newspeak", "talking through one's hat", "intimidation", and even "making supposed concessions" (Stelmach, 2018: 25-29). While doing so, they seem to disregard their preventive function, the primary aim of which is to eliminate threats. They make no efforts to comprehensively investigate the different causes of road incidents, including the behaviours underlying them. Hence, it would be an overstatement to say that the knowledge of the authorities about the aetiology of traffic crime is modest.

The study of practical experiences leads to a general conclusion that state authorities showed little interest in causes other than those attributable to the behaviour of traffic participants. For instance, they did not inquire into why the system failed to reveal mental diseases, alcohol/drug additions, aggressive tendencies, as well as other impairments, including those related to vision and hearing disorders, long reaction times, etc. Sporadically, some consideration was given to the accountability of state officers who did not react despite their knowledge of poor traffic organisation, markings and signage, road surface defects, or despite being aware that a driving license for motor vehicles had been issued to mentally ill, epileptic, visually impaired or otherwise impaired individuals.

An analysis of the causes of accidents or other road incidents leads to the conclusion that risky decisions creating specific hazards, were the determining factors. These decisions, however, mostly did not cause any danger. According to the author's research, criminal consequences ensued only in no more than 20% of all cases, although comprehensive research on the subject is yet to be conducted (Pawelec, 2020: 14). So far, no attempts have been made to identify signs of external behaviour preceding dangerous or risky decisions.

4 Impairments of psychomotor abilities and their causes – attempt at assessment

As far as objective elements are concerned, road traffic crimes and petty traffic offences essentially consist in violating the rules of cautious conduct, thereby putting legally protected rights of others at risk, and in leading to specific consequences, provided that such consequences are provided for by law. A violation of safety rules may involve behaviour that runs counter to a specific directive that prescribes a certain behaviour, or failure to behave as prescribed by such directive. Therefore, in addition to observing traffic regulations, traffic participants should exercise common sense, take general precautions and follow established uncodified rules (Pawelec, 2020: 77).

It should be noted that compliance with specific safety rules often requires reaction to atypical situations, provided that they were recognisable and foreseeable, and that there was sufficient time to take protective actions to eliminate the threat. Hence, it is extremely

important that the driver does not have impaired psychomotor reactions due to being intoxicated by alcohol or under the influence of psychoactive substances, and does not attempt to flee the scene, all of which are circumstances subject to harsher penalties and elements of a crime under Article 178s § 1 and Article 180 of the PC, as already mentioned. It should be remembered, however, that psychophysical properties, health status, drugs used, tiredness, skills, experience and other factors are all human-related (Pawelec, 2020: 134-148). They play an important role in safety, and their involvement in causing dangerous situations seems undebatable. Behaviours preceding dangerous situations can be identified by examining material from traffic cameras and CCTV cameras installed on buildings and other structures and fixtures. Such behaviours can be observed in drivers who are psychologically predisposed to being aggressive on the road, and even to display so-called "road rage".

Generally speaking, aggressive driving means driving a vehicle in a way that creates dangerous situations for others. It is manifested by excessive speed, ignoring traffic regulations, performing risky manoeuvres, disregarding other traffic participants, violating the give way rule, etc. Research has provided examples that the increased frequency of such behaviours is tantamount to the so-called road rage, which involves attacking other traffic participants physically, acting verbally aggressive towards them, and making non-verbal offensive gestures (Hołyst, 2019: 631-634).

In summary, it can be concluded that research on road aggression, considering its different dimensions and aspects, could, or rather should, represent an important first step towards improving prevention in road traffic. It is assumed – in fact, fairly commonly – that road aggression deserves special attention because it involves problems with interpersonal communication, limited by means of expression and interpretative ambiguity, that are not found elsewhere (Parkinson, 2001: 507-526; Hołyst, 2019: 636).

Research on road aggression – an increasingly common phenomenon, regrettably – considering its different dimensions and aspects, should lay the foundations for a concept that is relevant to preventing aggression, since it deserves special attention due to its involving problems with interpersonal communication, limited by means of expression and interpretative ambiguity, that are not found elsewhere (Hołyst, 2019: 636).

Clearly, considering road rage as the intentional violation of safety rules – which represents a highly aggravating circumstance – might prove a significant oversimplification. Indeed, aggression can be caused by various preparations that have little to do with psychoactive substances or alcohol. Among these is Boldeon – a substance used for muscle building and body sculpting. The users of this drug are not advised that it is an anabolic-androgenic steroid, classified in Group S1 of anabolic substances on the World Anti-Doping Agency's (WADA) List of Prohibited Substances and Methods. The Warsaw Anti-Doping Laboratory has noted that anabolic-androgenic steroids (AAS) cause a number of adverse effects, including mental symptoms, such as

mood swings, irritability, uncontrolled aggression, and other affective and mental symptoms and syndromes. For instance, this drug was detected, among others, in a person charged with uncontrolled aggression towards another traffic participant (Pawelec, 2020: 147).

5 Conclusion

Weakened psychomotor reaction, including a longer reaction time, can be caused not only by intoxication with alcohol or the effects of psychoactive substances, but also by factors that are altogether ignored during criminal proceedings, or in petty-offence cases, including, health status, tiredness, psychological attributes and personality features, and the use of certain drugs and preparations, even if they are legally marketed. Usually, the dangerous situations created by such drivers, which might lead to disasters, or cause the immediate danger of such disasters, may be preceded by atypical behaviours, specific, for instance, to mental diseases, associated with severe pulmonary diseases, balance disorders, eye disorders and other factors, including those associated with the use of certain drugs, as well as addictions.

According to the European Transport Safety Council, there has been little interest in these issues. The author has found clear evidence that the reports issued by the Road Traffic Office of the Polish National Police Headquarters do not mention the health status of traffic accident perpetrators, and also do not examine significant doubts as to the driver's health or qualifications. A similar situation applies to the Car Traffic Inspection. Meanwhile, an analysis was run in Finland of fatal road accidents in the years 2014-2018. Therein, it was found that in 16% of all cases, the driver's health status directly caused the tragic event. It is, therefore, worth undertaking work, in accordance with the EU Directive on driving licenses, to examine the psychomotor abilities of driver candidates. Particular attention should be paid to health issues related to poor vision, mobility impairment, cardiovascular diseases, diabetes, neurological diseases and obstructive pulmonary disease, epilepsy, mental disorders, alcohol issues, addiction to drugs and medications, as well as renal dysfunctions. Such examination should also be compulsory for drivers whose behaviour led to dangerous situations for other traffic participants. In such cases, they should be referred by traffic authorities – or by prosecutor's offices if crime is involved – to undergo specific medical examinations. Decisions in this regard should be subject to judicial control. In cases where dangerous situations have been documented, state authorities should take preventive measures following relevant regulations. After all, the main idea is to make sure that such behaviour does not lead to a crime. Hence, it seems reasonable to develop the aforementioned algorithm. Finally, efforts should be focused on preventing specific incidents instead of increasing repressive measures against consequences. Repressiveness is a road to nowhere, as we have yet to see comprehensive scientific research that would provide conclusive insights into the aetiology of road traffic crime.

References:

Bachrach, A. (1980) *Przestępstwa i wykroczenia drogowe w prawie polskim* (Warszawa: Wydawnictwo Naukowe PWN).
Hołyst, B. (2019) *Przestępstwa przeciwko życiu i zdrowiu* (Warszawa: Wolters Kluwer).
Parkinson, B. (2001) Anger on and off the road, *British Journal of Psychology*, 92, pp. 507-526.
Pawelec, K. (2017) *Sprowadzenie niebezpieczeństwa w ruchu drogowym* (Warszawa: Difin).
Pawelec, K. (2020) *Bezpieczeństwo i ryzyko w ruchu drogowym* (Warszawa: Difin).
Pawelec, K. (2021) *Zarys metodyki pracy obrońcy i pełnomocnika w sprawach przestępstw i wykroczeń drogowych* (Warszawa: Wolters Kluwer).
Stelmach, J. (2018) *Sztuka manipulacji* (Warszawa: Wolters Kluwer).

Procedure for the Identification of an Operator of Essential Services under the Act on the National Cybersecurity System

DOROTA LEBOWA

Abstract The Polish Act on the National Cybersecurity System defines cybersecurity as "the resistance of information systems to activities that violate the confidentiality, integrity, availability and authenticity of the data processed or related services offered by these systems". The Act is designed to ensure an adequate level of protection for users of digital services, and one of the basic measures to achieve this is to impose numerous obligations on digital service operators. The Act on the National Cybersecurity System sets out a procedure for identifying an entity as providing essential services. Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, concluded with an administrative decision. The provisions of the Polish Code of Administrative Procedure apply to the procedure for identifying an operator of essential services.

Keywords: • cybersecurity • operator of essential services • administrative decision • essential service

CORRESPONDENCE ADDRESS: Dorota Lebowa, Ph.D., Assistant Professor, Maria Curie-Sklodowska University, Faculty of Law and Administration, Department of Administrative Law and Administrative Sciences, Plac Marii Curie-Sklodowskiej 5, 20-031 Lublin, Poland, e-mail: dorota.lebowa@mail.umcs.pl, ORCID: 0000-0003-3316-5541.

https://doi.org/10.4335/2022.1.10 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The ever-growing influence of information and communication technology (ICT) on the socio-economic development of the Member States of the European Union and the increased use of ICT results in the products and services offered being increasingly dependent on cybersecurity (Karpiuk, 2021a: 611). The extensive architecture of ICT systems, including big data operations, serves the development of communication, trade and transport, and provides a foundation for rendering essential, digital and public administration services. Unfortunately, the opportunities offered by modern digital technologies are also used for unfair competition practices, to interrupt the continuity of selected services (whether for hooliganism purposes or to undermine the competitive position of an entity), to commit crimes using the Internet, or to carry out terrorist activities (explanatory memorandum to the government-proposed draft Act on the National Cybersecurity System, Sejm Papers no. 2505).

The Act of 5 July 2018 on the National Cybersecurity System (consolidated text: Journal of Laws of 2020, item 1369), hereinafter referred to as ANCS, implements Directive 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. Pursuant to the principles of the so-called pro-EU interpretation of national law (see, for example, the CJEU judgment of 9 March 2004, in joined cases C 397/01 to C 403/-1, Pfeiffer, 2004, p. I-8835, paragraph 113), it is right and necessary to refer to the relevant provisions of the Directive when interpreting individual norms of the ANCS. Important guidelines on how to understand the objectives of the Directive are provided in its preamble, which points out that networks and information systems and services play an important role in society. Their reliability and security are essential for economic and social activities and especially for the functioning of the internal market. The scale, frequency and impact of security incidents are larger and larger and pose a serious threat to the functioning of networks and information systems (Hydzik, 2019: 84-87).

The definition of operator of essential services is contained in Article 4(4) and Article 5(2) of the NIS (Network and Information Security) Directive 2016/1148 of 6 July 2016, according to which ‘operator of essential services’ means a public or private entity of a type referred to in Annex II, which provides a service which is essential for the maintenance of critical societal and/or economic activities; the provision of that service depends on network and information systems; and an incident would have significant disruptive effects on the provision of that service (Karpiuk, 2021b: 238).

The *ratio legis* behind the ANCS is to protect users of digital services in a broad sense from negative exposure to risks associated with the lack of an adequate degree of cybersecurity (Wajda, 2020: 5). The correct implementation by operators of essential services of the obligations imposed on them by the Act should, as planned by the lawmakers, translate into an appropriate degree of protection in the space of digital

services. These obligations comprise a very broad and complex range of activities concerning, among other things, the obligation to implement systemic solutions for managing security in the information system, the obligation to designate appropriate structures responsible for cybersecurity, information obligations (in relation to users and relevant authorities), obligations to implement appropriate procedures in the area of cybersecurity, including in the area of incident response, and the obligation to conduct audits in the area of cybersecurity (Chałubińska-Jentkiewicz, Karpiuk & Kostrubiec, 2021: 16). The implementation of these obligations is secured by the mechanism provided for in the ANCS for the supervision of their implementation, as well as administrative liability, i.e. the power to impose administrative penalties by competent authorities.

To sum up, it can be stated that the legislature has set very strict requirements for operators of essential services, which may entail the need to rebuild the company structure and a new division of powers and responsibilities in order to ensure an appropriate degree of cybersecurity (Sawicki, 2019: 13-20). Hence, the procedure established in the ANCS for identifying an entity as a provider of essential service is so important.

2 Procedure for the identification of operator of essential service

Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, concluded with an administrative decision. The procedure for identifying an operator of essential services is generally governed in Poland by the provisions of the Act of 14 June 1960 the Code of Administrative Procedure (consolidated text: Journal of Laws of 2021, item 735, as amended), hereinafter referred to as CAP. The Act on the National Cybersecurity System does not contain a direct reference to the provisions of the CAP. It seems that such a reference is not necessary in the light of the principles of correct lawmaking, On the other hand, the application of the provisions of the CAP is indicated by the reference to the detailed regulation concerning the time limits for settling administrative matters contained in Article 5(5) ANCS (the period for consultation referred to in paragraph 4 shall not be included in the time limits referred to in Article 35 of the Act of 14 June 1960 - Code of Administrative Procedure). Moreover, the requirements for the application of the provisions of the CAP on jurisdictional proceedings set out in Article 1(1) CAP (the Code of Administrative Procedure governs proceedings before public administration bodies in individual matters falling within the jurisdiction of these bodies, resolved through administrative decisions or settled on a tacit basis) must be met, and proceedings in this matter have also not been explicitly excluded from the application of the Code in Articles 3 and 4 CAP or in specific provisions of the Code.

The Act provides for a specific procedure for the competent authority to determine whether the entity concerned meets the conditions to be considered an operator of essential services. The authority may request a specific entity to provide information allowing for a preliminary assessment of whether the entity meets the conditions to be

considered as an operator of essential service (Article 43ANCS). Such a solution stems from a very large number of entities that need to be verified. The procedure is deformalised and shall take place without initiating administrative proceedings. This is an exception to the fundamental principle of administrative law, namely the running of jurisdictional proceedings to concretise the legal norm and to determine the rights and obligations of supervised entities. Such a basic procedure in the Polish legal system is the administrative procedure carried out on the basis of the Code of Administrative Procedure. The competent authority requests the entity by way of a simple official letter containing the questions which will allow an initial assessment whether it would be appropriate to initiate the formal procedure. The request should specify a time limit to provide the requested information, which must not be less than 14 days. The addressee of the letter is not obliged to provide information. However, it should be pointed out that the entity concerned may be interested in providing that information to avoid the initiation of an administrative procedure, if the preliminary proceeding demonstrates that the statutory conditions for considering the entity as an operator of essential service are not met. The information provided by the entity will be able to be used as evidence in future administrative proceedings.

As a rule, the administrative procedure for identification is initiated *ex officio*. However, the provisions of the Code of Administrative Procedure do not prevent another authority whose competence includes cybersecurity issues from drawing the competent authority's attention to the need to initiate such proceedings. As part of its business, an important piece of information for the entity running such business is the possibility of excluding it from the requirements of the ANCS. It is therefore possible that an entity not recognised as an operator of essential services may apply for such proceedings. The ANCS also does not exclude the possibility of initiating such proceedings at the request of an NGO or allowing this organization to participate in ongoing proceedings with the rights of a party, if it is justified by the statutory objectives of this organization and if there is a public interest in doing so (Article 31 §1(1) CAP).

The public administration body is not obliged to issue a separate decision on the initiation of proceedings. The initiation of proceedings *ex officio* entails, in the light of Article 61 § 4 CAP, the obligation to notify all the parties of this initiation. The case-law stresses that the notification of the initiation of proceedings served to a party is not a value in itself, but has a specific purpose, namely primarily to inform the parties that an administrative procedure has begun in which they may need to defend their rights (Judgment of the Supreme Administrative Court of 18 April 2008, case ref. no. II OSK 429/07, LEX no. 469206). On the other hand, when a party is served the notice of initiation of proceedings, the Code requirements for the public administration body to conduct proceedings under and within the limits of law are applicable, taking into account the constitutional principles and general administrative procedural principles.

The Act does not provide for a time limit to conclude the administrative procedure for the adoption of an identification decision. Therefore, in this respect, reference should be made to the time limits contained in the CAP. The handling of a case requiring clarification proceeding should take place no later than one month and for a particularly complex case no later than two months after the initiation of the proceedings (Article 35 § 3 CAP).

The procedure for identifying an operator of essential services may be concluded with a decision to recognise it an operator of essential services only if the competent authority has determined that the entity meets the conditions for obtaining this status (of a systemic and substantive nature). If, on the other hand, following clarification proceeding, the authority finds that the conditions for considering an entity to be an operator of essential services are not met, the procedure should also end with an administrative decision. The provisions of the ANCS do not contain a separate regulation in this matter, so the authority in such a situation should issue a decision to discontinue the proceedings pursuant to Article 105 § 1 CAP.

According to Article 7 CAP, in the course of the proceedings, public authorities must safeguard the rule of law, take all necessary steps, either *ex officio* or at the request of the parties, to examine the facts thoroughly and to settle the case having regard to the public interest and the legitimate interests of citizens. This provision expresses the principle of objective truth, according to which a public authority is required to study thoroughly all the facts in order to examine the case correctly, which is a necessary element in the proper application of a norm of substantive law. This principle is mainly guaranteed by the rules governing evidence taking. The authority is required to collect thorough evidence and therefore to take a series of procedural steps to gather and consider all the evidence (Article 77 § 1 CAP). In the course of the proceedings, it is also necessary to take account of the principle of active participation of the parties in the proceedings by providing the parties with access to the file of the case and by notifying them of the opportunity to comment on the evidence collected and the service of the decision.

3 Conditions for considering an entity as an operator of essential services

The following entities shall be deemed operators of essential services: 1) those which are listed in the annex to the ANCS and have an organisational unit in the territory of the Republic of Poland; 2) which provide an essential service specified in the list of essential services; 3) the provision of this service depends on information systems; 4) an incident would have a significant disruptive effect on the provision of the essential service by this operator (Article 5(1) and (2) ANCS).

Specific categories of entities are described in the annex to the ANCS to indicate potential entities for which a decision to recognise them as operators of essential services may be issued now or in the future, but this does not mean that such an entity will be automatically

recognised as an operator of essential services. Essential service within the meaning of Article 2(16) of the Act under is a service which is of key importance for maintaining a critical social or economic activity, specified in the list of essential services. The list is contained in the Ordinance of the Council of Ministers of 11 September 2018 on the list of essential services and the thresholds of significance of the disruptive effect of an incident on the provision of essential services (Journal of Laws of 2018, item 1806). For an entity to be qualified as an operator of essential service, it is necessary that the provision of the essential service is dependent on information systems. Information system is defined in Article 2(14) ANCS as an ICT system referred to in Article 3(3) of the Act of 17 February 2005 on computerisation of the activities of public task-performing entities (consolidated text Journal of Laws of 2021, item 670) together with data in electronic form processed in it. The case law points out that information system is a set of cooperating IT devices and software ensuring the data processing (including storage, as well as sending and receiving) by telecommunication networks by means of a telecommunications device appropriate for a given type of network and designed to be connected directly or indirectly to network terminals, together with the data processed in it in electronic form (Judgment of the Regional Administrative Court of 5 August 2020, VI SA/Wa 2667/19, LEX No. 3068097). In general, therefore, the dependence of the provision of an essential service on information systems should be referred to such circumstances in which the use of information systems is necessary for the continuous and effective provision of the service in question.

The last condition for an entity to be considered an operator of essential services is related to the fact that a cybersecurity incident, if any, has a significant disruptive effect on the provision of the essential service by the entity. Cybersecurity is understood as the resistance of information systems to activities that compromise the confidentiality, integrity, availability and authenticity of the data processed or related services offered by these systems (Article 2 (4) ANCS). According to Article 2(5) ANCS, incident is an event that has or may have an adverse impact on cybersecurity. It is not sufficient for an entity to provide an essential service in a manner that is dependent on information systems, but it is further required that a possible incident affects (or could affect) the confidentiality, integrity, availability and authenticity of the data processed for the provision of the service or affects the provision of that service (e.g. interferes with its proper provision or even prevents its performance).

What is legally relevant is not any impact of an incident on the provision of a service, but rather causing an effect of a material nature that disrupts the provision of this service by a given operator, e.g. one that affects continuity of provision of the service, quality of the service, security of users, protection of users' data, etc. The degree of significance of the incident is of a highly arbitrary nature. Possible effects of such an incident may depend on many variables, such as the scale of provision of a given type of service, or the scale of impact of the incident on economic or social activity. That is why it was necessary to establish thresholds of significance of the disruptive effect, on the basis of which the

competent authorities assess, in the course of the procedures for identification of operators of essential services, the significance of the disruptive effect for a given service provided by a particular operator. These thresholds are set out in the aforementioned Ordinance of the Council of Ministers of 11 September 2018 on the list of essential services and the thresholds of significance of the disruptive effect of an incident on the provision of essential services.

The disruptive effect significance thresholds are set out in the Annex to the Ordinance for each essential service sector. In general, these thresholds correspond to the cross-sectoral factors set out in the provisions of 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. As follows from Article 6(1) of the Directive, when determining the significance of a disruptive effect, Member States must take into account at least the following cross-sectoral factors: 1) the number of users relying on the service provided by the entity concerned; 2) the dependency of other sectors referred to in Annex II on the service provided by that entity; 3) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; 4) the market share of that entity; 5) the geographic spread with regard to the area that could be affected by an incident; 6) the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

4 Decision on recognising an entity as an operator of essential service

The recognition as an operator of essential service is to be done by way of an administrative decision. Administrative decision means a specific administrative act, which is a manifestation of the will of public authorities administering the State, issued under generally applicable administrative law of a sovereign and external nature, resolving a specific case of a specific natural or legal person, in proceedings governed by procedural rules (Judgment of the Supreme Court of 3 April 2000, I CKN 582/98, LEX No. 50843; Zdyb, Stelmasiak 2020: 220-224). The constituent elements of administrative decision are listed in Article 107 CAP. This provision obliges the authority to clarify all relevant factual and legal circumstances and to explain to the party the reasons behind the decision on handling the party's request. The statement of reasons for the decision must be drafted in such a way as to make it possible to understand the body’s reasoning and to review correctness of the decision. A precondition for the recognition as an operator of essential services is that all the above-mentioned conditions must be met cumulatively, which should be reflected in the factual and legal substantiation for the decision. The legal basis for the decision in question should be the following provisions: Article 5 1 ANCS (systemic condition), Article 5 (2) ANCS (substantive condition) and Article 41(1) and Article 42 (1) item 2 ANCS (competent authority).

Factual findings should concern all the conditions for the recognition as an operator of essential service. The competent authority may not confine itself to identifying the evidence gathered in the case and referring to the content of the provisions applicable to the case. It is also necessary to establish and demonstrate a link between various conditions, in particular regarding the provision of a particular service, with the fact that it depends on the functioning of the information system, or to analyse the significance of the disruptive effect.

As a rule, a decision must not be enforced before the time limit for lodging an appeal against it, and lodging an appeal suspends its enforcement. However, the legislation provides for quite numerous exceptions to this rule. This is because a decision may be subject to the obligation of immediate enforceability by virtue of law or where the requirement of immediate enforceability is conferred on it by a public administration body pursuant to Article 108 CAP. "The state of immediate enforceability of a decision" consists in the possibility of immediate enforceability of the decision, which becomes an enforcement order, despite being not final (judgment of the Supreme Administrative Court of 7 December 2018, I OSK 3311/18, LEX No. 2628876). Article 5 (7) ANCS indicates that the decision on recognition of an entity as an operator of essential services is subject to immediate enforcement. Contrary to the literal wording of the Act, it should be assumed that the decision is not immediately enforceable by operation of law, but the competent authority is obliged to declare *ex officio* the decision on recognition as an operator of essential service immediately enforceable (Besiekierska, 2019). However, the immediate enforceability of a decision does not mean that the obligations imposed by the Act on the operator are promptly applicable. The individual obligations imposed by the law are to be fulfilled by the operator within the time limits set out in Article 16 ANCS: from 3 months to a year from the date of service of the decision. The essence of this solution is to oblige operators of essential services to undertake performing the obligations imposed by the ANCS as soon as possible (Wajda, 2020: 9). It is the right solution from the point of view of clients of these services since the operator, regardless of filing the appeal to the administrative court, will be required to ensure the provision of services with an appropriate degree of cybersecurity.

An entity recognised in the decision as an operator of essential services may appeal against the decision to an administrative court. A party dissatisfied with the decision of the body may also exercise the right provided for in Article 127 § 3 CAP, according to which a decision issued in the first instance by the Minister may not be appealed against, but a party dissatisfied with the decision may apply to this body for reconsideration of the case; the provisions on appeals against decisions shall apply accordingly to such an application. The relevant case law indicates that in the proceedings for reconsideration of the case, similarly as in appeal proceedings, the administrative body is obliged to reconsider the case in its entirety, including in particular to respond to the allegations and arguments contained in the request for reconsideration (judgment of the Supreme Administrative Court of 19 March 2019, II OSK 1132/17, LEX No. 2655883). In the

ANCS, the legislature also regulated a situation similar to the regulation contained in Article 162 CAP, i.e. declaring a decision expired due to its groundlessness. In relation to an entity which no longer meets the conditions for being recognised as an operator of essential services, the competent authority for cybersecurity makes a decision stating that the decision on recognition as an operator of essential services has expired (Article 5(6) ANCS). The proceedings in this matter may be initiated *ex officio*, but in practice this is most often done at the request of an interested entity.

5 Conclusion

The cybersecurity obligations contained in the Act on the National Cybersecurity System concern, *inter alia*, the implementation of an effective security management system, including risk management, procedures and mechanisms for reporting and handling incidents or organisation of structures at operator level. However, the annex to the Act lists potential categories of entities in particular sectors of the economy and government activities, from which operators of essential services may be selected through an administrative decision. The criteria for identifying operators of essential services set out in the Act on the National Cybersecurity System meet the requirements referred to in Directive 2016/1148. Recognition of a specific entity as an operator of essential services takes place through a formalized procedure with specific guarantees, based as a rule on the provisions of the Code of Administrative Procedure.

References:

Besiekierska, A. (ed.) (2019) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warszawa: C.H. Beck).

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.

Hydzik, W. (2019) Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych, *Przegląd Ustawodawstwa Gospodarczego*, 3, pp. 84-87.

Karpiuk, M. (2021a) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-government*, 19(3), pp. 609-620, https://doi.org/10.4335/19.3.609-620(2021).

Karpiuk, M. (2021b) The organisation of the national system of cybersecurity. Selected issues, *Studia Iuridica Lublinensia*, 30(2), pp. 233-224, http://dx.doi.org/10.17951/sil.2021.30.2.233-244.

Sawicki, M. (2019) Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego, *Europejski Przegląd Sądowy*, 9, pp. 13-20.

Wajda, P. (2020) Cyberbezpieczeństwo – sektorowe aspekty regulacyjne, *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, 2, pp. 9-27.

Zdyb, M. & Stelmasiak, J. (eds.) (2020) *Prawo administracyjne. Część ogólna, ustrojowe prawo administracyjne, wybrane zagadnienia materialnego prawa administracyjnego* (Warszawa: Wolters Kluwer).

Supervision and Inspection in the Field of Cybersecurity

MAŁGORZATA CZURYK

Abstract The national cybersecurity system consists of a number of entities that play important roles in protecting cyberspace from threats, including those compromising the normal functioning of the state. The national cybersecurity system aims to ensure national cybersecurity, including the uninterrupted provision of critical and digital services, by achieving an adequate level of security within the information systems used to provide these services and ensuring incident handling. Supervision and inspection in terms of compliance with security requirements covers providers of cybersecurity services, operators of essential services, as well as digital service providers.

Keywords: • supervision • inspection • cybersecurity • essential service • digital service

CORRESPONDENCE ADDRESS: Małgorzata Czuryk, Ph.D., Dr. Habil., University Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, ul. Obitza 1, 10-725 Olsztyn, Poland, e-mail: malgorzata.czuryk@uwm.edu.pl, ORCID: 0000-0003-0362-3791.

https://doi.org/10.4335/2022.1.11 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Cybersecurity can be seen in both public and private aspects. The development of information technologies has, on the one hand, resulted in much greater opportunities for the rapid acquisition, transmission, or collection of information, while on the other hand, new threats have arisen that occur in cyberspace. In view of the great importance of ICT systems and networks, both for the economic and public sphere, the state must have appropriate tools to combat cyberattacks, especially those that are relevant to its functioning. It is the purpose of supervision and inspection to prevent unwanted incidents in cyberspace, thus ensuring cybersecurity at an appropriate level and allowing the uninterrupted performance of public tasks. The ideal state of being free of all disruptions is not achievable, so the realistic objective is to ensure a level of cybersecurity that allows public needs to be met uninterruptedly, while maintaining appropriate quality standards and adequate availability of services at optimal cost of service provision.

Cybersecurity involves the prevention of threats, their anticipation, as well as the removal of consequences arising from their occurrence. The sphere in which such threats and threat outcomes occur is cyberspace (Karpiuk, 2021a: 612). According to Article 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended) – the Act is hereinafter referred to as the 'NCSA', cybersecurity is the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. As information systems develop, an adequate protective infrastructure must also be created to ensure security in cyberspace.

Nowadays, cybersecurity is very important, and the consequences of actions that undermine this type of security are experienced not only in the public sphere, but also in the economic and social spheres. Therefore, the state must react quickly and decisively to cyberattacks by looking for ever more modern protection mechanisms (among other actions). Responding to the increasingly frequent threats to cyberspace, the legislators have decided that an appropriate legal regulation is necessary, allowing for both a proper diagnosis and an adequate response in the event of cyberattacks (Karpiuk, 2021b: 234). In today's highly computerised world, in addition to the activities of public entities in ensuring the security of various resources, technical protection is increasingly needed (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 52).

Under the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Polish Journal of Laws of 2020, item 1369, as amended), supervision and inspection applies to operators of essential services, digital service providers and providers of cybersecurity services, and it is these aspects that the analysis will focus on. An essential service, according to Article 2(16) of the NCSA, is a service that is deemed essential in maintaining critical social or economic activity and which is included on the list of essential services. A digital service, according to Article 2(15) of the NCSA, is an

electronically supplied service. Provision of an electronically supplied service is, according to Article 2(4) of the Act of 18 July 2002 on Providing Services by Electronic Means (consolidated text, Polish Journal of Laws of 2020, item 344, as amended), the performance of a service rendered without the simultaneous presence of the parties (at a distance), through the transmission of data at the individual request of the customer, sent and received by means of electronic processing devices, including digital compression and data storage, which is entirely broadcast, received or transmitted via a telecommunications network. At the same time, telecommunications networks, pursuant to Article 2(35) of the Act of 16 July 2004 – Telecommunications Law (consolidated text, Polish Journal of Laws of 2021, item 576, as amended), should be understood as transmission systems and switching or routing equipment, as well as other resources, including inactive network elements, that enable the broadcasting, reception or transmission of signals by wire, radio, optical or other electromagnetic means, regardless of their type.

2 The concept of supervision and inspection

The concept of supervision should be understood as such shaping of mutual relations between public administration entities, in which the supervisory entity has the power to directly interfere with the activities of the supervised entity (Polinceusz, 2013: 312). Supervision is an institution that enables authoritative interference in the sphere of activity of the supervised entity when irregularities are detected. The criteria, as well as the supervisory authorities, and the scope of supervision must be clearly specified by the legislators. It cannot be presumed that there is any authoritative interference with the sphere of independence of supervised entities; such interference must be clearly provided for in statutory-grade generally applicable laws. If there is no clear legal basis for initiating the supervisory procedure, it is not permissible.

The concept of inspection is a multidimensional term that applies to all forms of organisation of social life, therefore it can be used in various semantic contexts (Kostrubiec, 2013: 329). The purpose of inspection – as provided for in Article 3 of the Act of 15 July 2011 on Inspection in State Administration (consolidated text, Polish Journal of Laws of 2020, item 224, as amended) – the Act is hereinafter referred to as the 'ACSA' – is to assess the activity of the inspected entity on the basis of established facts, subject to the adopted inspection criteria. Where irregularities are found, the purpose of inspection is also to determine their extent, causes and effects, as well as those responsible, and to formulate recommendations aimed at correcting the irregularities. Inspection can be conducted under an ordinary and simplified procedure. It should be emphasised, however, as provided for in Article 51(1) of the ACSA, that inspection can be ordered in a simplified procedure in cases justified by the nature of the case or urgency of inspection activities.

3 Supervision in the field of cybersecurity

The issues of supervision in the application of the provisions of the NCSA, therefore, in the field of cybersecurity, are set out in Article 53 of the NCSA. This supervision, according to Article 53(1) of the NCSA, is exercised by: 1) the minister competent for computerisation in respect of the fulfilment by the providers of cybersecurity services of the requirements concerning: a) the fulfilment of organisational and technical conditions making it possible to ensure cybersecurity to the served operator of an essential service; b) the possession of premises for the provision of incident response services, protected from physical and environmental threats; c) the application of a safeguard to ensure confidentiality, integrity, availability and authenticity of the processed information, taking into account personal security, operation and architecture of the systems; 2) the competent authorities for cybersecurity with regard to: a) fulfilment by operators of essential services of their obligations under the Act with respect to countering cybersecurity threats and reporting serious incidents; b) compliance by providers of cybersecurity services with the security requirements of their services and performance of their obligations with respect to reporting major incidents; this concerns both the application of appropriate technical and organisational measures, acting on the basis of risk analysis, identifying threats, or proper management of ICT networks and systems.

Pursuant to Article 41 of the NCSA, the competent authorities for cybersecurity, who also exercise supervision, include: 1) for the energy sector – the minister competent for energy; 2) for the transport sector, excluding the water transport sub-sector – the minister competent for transport; 3) for the water transport sub-sector – the minister competent for the maritime economy and the minister competent for inland navigation; 4) for the banking sector and financial markets infrastructure – the Polish Financial Supervision Authority; 5) for the healthcare sector – the minister competent for health; 6) for the healthcare sector and the digital infrastructure sector covering entities subordinated to the Minister of National Defence or supervised by him and enterprises of special economic and defence importance in respect of which the Ministry of National Defence is the authority organising and supervising the performance of tasks for state defence – the Minister of National Defence; 7) for the drinking water supply and distribution sector – the minister competent for water management; 8) for the digital infrastructure sector and digital service providers – the minister competent for computerisation. As a rule, therefore, the supervisory authorities are ministers in charge of a specific department of government administration, only in the case of the banking sector and financial market infrastructure is it the Polish Financial Supervision Authority.

As part of the supervision of operators of essential services, digital service providers and providers of cybersecurity services, pursuant to Article 53(2) of the NCSA: 1) the competent authority for cybersecurity or the minister competent for computerisation exercises inspection on compliance with security requirements and obligations in this respect; 2) the competent authority for cybersecurity imposes fines on operators of essential services and digital service providers. Supervision in the field of cybersecurity

is carried out in two stages: first, inspection is conducted, covering the performance of obligations on countering cybersecurity threats and reporting incidents, as well as meeting requirements to ensure cybersecurity, including the security of digital services provided. Where irregularities are found, the competent authority for cybersecurity may impose a fine on the supervised entity. In the case of a digital service provider, a fine is imposed upon evidence that it fails to comply with the security requirements of the digital services provided or the statutory obligations regarding the reporting of material incidents.

4 Cybersecurity-related inspection

If the inspection concerns an entity that is an entrepreneur, pursuant to Article 48 of 6 March 2018 – the Entrepreneurs Law (consolidated text, Polish Journal of Laws of 2021, item 162, as amended) – the Act is hereinafter referred to as the "EL" – the inspection authority notifies the entrepreneur of its intention to initiate an inspection. The inspection is initiated no sooner than after 7 days and no later than after 30 days from the date of delivery of the notice on the intention to initiate inspection. At the request of the entrepreneur, inspection may be initiated within 7 days from the date of delivery of the notice. If inspection is not initiated within 30 days from the delivery of the notice, the initiation of the inspection requires a new notice. The lack of a notice of inspection undoubtedly has a significant impact on the inspection's outcome. It prevents the entrepreneur from proper preparation for the inspection activities. Nevertheless, since the law stipulates that an effective notice is a necessary condition for conducting inspection, prior to its initiation, the inspecting entity is obliged to have evidence of delivery of a relevant notice to the entrepreneur (judgement of the Voivodeship Administrative Court in Warsaw of 25 October 2017, VI SA/Wa 1122/17, LEX No. 2425534). A notice of the intention to initiate inspection is not issued, among others, in the event when: 1) inspection is to be conducted in accordance with the ratified international agreement or directly applicable provisions of the European Union law; 2) the inspection must be conducted to prevent an crime or petty offence, a fiscal crime or a fiscal petty offence, or to secure the evidence that such offence or crime has been committed; 3) the inspection is justified when there is a direct threat to life, health or the environment; 4) the entrepreneur does not have the address of residence or the registered address, or the delivery of letters to the given addresses was ineffective or difficult.

It does not follow from the regulations that the inspection authority, in explaining the reasons for an inspection without prior notice, is required, at the moment of its initiation, to provide the justification for accepting such a basis for inspection, indicating why such inspection is, for example, essential to prevent the commission of an crime or a petty offence, a fiscal crime or a fiscal petty offence, or to secure the evidence of its commission. In view of these considerations, it seems hardly justified to warn the inspected entity about the evidence that the authority will look for as part of the initiated proceedings. Therefore, the citation of the relevant legal basis should be treated as sufficient (judgement of the Supreme Administrative Court of 28 September 2017, I FSK 1125/17, LEX No. 2404466). The list of exemptions from the obligation to notify about

the inspection indicates that the legislators included it in special cases, related to the protection of particularly socially sensitive goods, where the balance of the entrepreneur's interest related to the possession of information about the planned inspection and the protection of these goods by the inspection authorities speaks in favour of the primacy for the protection and possibly rapid response to threats or pathologies. And it is indisputable here that the inspection authority, within the scope of its competence, may act ex officio and the source from which the authority obtained information about the threat is of no significance (judgement of the Supreme Administrative Court of 29 December 2015, II OSK 1001/14, LEX No. 1999995).

A person conducting inspection related to entities that operate as businesses – as provided for in Article 55 of the NCSA – has the right to: 1) freely enter and move around the premises of the inspected entity without the obligation to obtain a pass; 2) access documents related to the activity of the inspected entity, collect against a receipt and secure documents related to the scope of inspection, while observing the provisions on legally protected secrets; 3) prepare, and if necessary request the preparation of, copies, excerpts or extracts of documents, as well as statements or calculations indispensable for the inspection; 4) process personal data as needed for the achievement of the inspection objective; 5) request to provide oral or written explanations in matters related to the scope of inspection; 6) perform the visual inspection of devices, carriers and information systems. These are the standard inspection powers that make it possible to verify the facts and identify possible irregularities.

Article 56 of the NCSA imposes obligations on inspected entrepreneurs that make it possible to conduct inspections efficiently. Inspected entities that are entrepreneurs provide the inspecting person with the conditions necessary to efficiently conduct the inspection – in particular, by ensuring the immediate presentation of requested documents, providing oral and written explanations in a timely manner in matters covered by the inspection, providing access to the necessary technical equipment, as well as making copies or printouts of documents and information collected on carriers, in devices or in information systems on their own. The inspected entity certifies copies or printouts as true copies of the originals. In the event of refusal to certify consistency with the originals, they are confirmed by the inspecting person, who makes a note about this fact in the inspection report. Without access to documentation or explanations from the entrepreneur, it may prove impossible to conduct the inspection. Therefore, the legislators have imposed an obligation on the inspected entity to immediately present the requested documents, provide oral and written explanations in a timely manner, as well as to make the necessary technical equipment available, or to make copies or printouts of documents. It should be emphasised, however, that all these obligations may not go beyond the scope of the inspection, i.e. the inspection authority may not demand more information than required by the scope of the inspection.

The details of the inspection are documented in a report. Pursuant to Article 58 of the NCSA, the person inspecting entities that are entrepreneurs shall present the details of the

inspection in a inspection report. An inspection report provides: 1) the name or first name and surname and address of the inspected entity; 2) the first name and surname of the person representing the inspected entity and the name of the body representing this entity; 3) the first name and surname, position and authorisation number of the inspecting person; 4) the start and end dates of inspection activities; 5) the subject and scope of the inspection; 6) the facts established in the course of the inspection and other information essential for the conducted inspection, including the scope, reasons and effects of the irregularities found; 7) attachments, if any. This is the basic information that makes it possible to take relevant decisions at a later stage, particularly to identify irregularities and persons responsible for them, especially if it proves necessary to take appropriate punitive measures against the inspected entity.

A inspection report is signed by the inspecting person and the person representing the inspected entity. Prior to signing the report, the inspected entity may, within 7 days from the date of its presentation for signing, make written reservations to the report. If reservations are made, the inspecting person analyses them and, if necessary, takes additional inspection steps. In the event that the reservations are justified, the inspecting person changes or supplements the relevant part of the report in the form of an annex to the report. In the event that the reservations are not accepted in whole or in part, the inspecting person informs the inspected entity in writing. A reservation may not be made after the inspection report has been signed. The inspecting person makes a note on the refusal to sign the report, including the date of such refusal. The report in paper form is drawn up in two copies, one of which is left for the inspected entity, and if the report is drawn up in electronic form, it is delivered to the inspected entity.

Pursuant to Article 51 of the EL, the inspection is conducted in the entrepreneur's registered office or place of business, and during working hours or at the time of the actual performance of business activity by the entrepreneur. Upon the entrepreneur's consent or request, the inspection is conducted in the place where documentation, including tax books, is stored other than the registered office or place of business to facilitate the inspection. With the consent of the entrepreneur, the inspection, or individual inspection activities, may also be conducted in the registered office of the inspection authority to facilitate the inspection. Subject to the entrepreneur's consent, the inspection, or individual inspection activities, may be conducted remotely via a postal operator or by electronic means of communication, if this serves to facilitate the inspection or is justified by the nature of the business activity conducted by the entrepreneur. If, in cases requiring the consent or request of the entrepreneur, the inspection authority undertook inspection activities without such consent or request, the documents and information collected in the course of such activities do not constitute evidence in the inspection proceedings.

Inspection activities should be performed in an efficient manner and in such a way as not to disturb the functioning of the entrepreneur's business. In the event that the entrepreneur indicates in writing that the performed activities significantly interfere with the entrepreneur's business activity, the necessity to undertake such activities shall be

justified in the inspection report. This rule is introduced by Article 54 of the EL. The purpose of the entrepreneur's activity is to conduct business, and the inspection may not lead to the suspension of the business activity – it may limit it, but only to the extent necessary to achieve the objective of the inspection. The inspection may not be excessive, and it should create as little burden for the entrepreneur as possible.

If deficiencies are identified, the inspection authority may issue follow-up recommendations to the inspected entity. Pursuant to Article 50 of the NCSA, if, on the basis of the information contained in the inspection report, the competent authority for cybersecurity or the minister competent for computerisation recognises that there may have been a breach of the provisions of the NCSA by the inspected entity, it will issue follow-up recommendations concerning the removal of irregularities. The follow-up recommendations may not be appealed against. The inspected entity is required, within the prescribed time limit, to inform the competent authority for cybersecurity or the minister competent for computerisation on the manner in which the recommendations have been implemented.

5 Conclusion

Supervision and inspection related to cybersecurtiy (and other areas) is exercised and conducted by the authorities expressly mentioned by the legislators, including in the NCSA. Supervisory and inspection powers may not be presumed due to the onerousness of these measures for the the entities that are supervised and inspected. Specific solutions in this regard are provided in Article 60 of the EL, on the basis of which the executive body of a municipality may take actions aimed at suspending the entrepreneur's business activity, including if it does not meet the conditions provided for ensuring cybersecurity, and, at the same time, leads to qualified threats. Pursuant to this provision, in the event that a threat to life or health, danger of substantial damage to property or a direct threat to the environment is identified as a result of the performance of this activity, the commune head or the mayor of the city must immediately notify the competent authorities – in this case, the competent authorities competent cybersecurity, as set out in the NCSA. The notified authorities shall immediately apprise the commune head or the mayor of the city of the actions taken. Should it be impossible to inform the competent authorities, the commune head or the mayor of the city may order the entrepreneur, by way of a decision, to suspend business activity for a necessary period of time, not longer than three days. The decision ordering the suspension of business activity in the event of a threat to life or health, danger of substantial damage to property or a direct threat to the environment as a result of the performance of such activity is immediately enforceable. The entrepreneur's business activity may be suspended where the entrepreneur fails to comply with their obligations with respect to countering cybersecurity threats and incident reporting and where, at the same time, this has led to a threat to life or health, danger of substantial damage to property or a direct threat to the environment.

The tasks to be completed by the inspection should be specified in terms of the functioning of the entire cybersecurity system. An effective inspection system should contribute to ensuring that the implementation processes run properly and that the best possible results are achieved in each activity. Several elements contribute to the effectiveness of inspection activities. One is the proper selection of the subject matter of the inspection. Professionalism of the inspection is also important. This term should be understood as the due preparation of the inspectors, both substantive and ethical (Nowikowska, 2021: 100). Professionalism is the element of the inspection that is manifested in the substantive and organisational preparation of the inspecting entity, whose employees have sufficient knowledge and experience (Kostrubiec, 2013: 331).

References:

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

Karpiuk, M. (2021a) The Local Government's Position in the Polish Cybersecurity System, *Lex Localis – Journal of Local Self-Government*, 3, pp. 609-620, https://doi.org/10.4335/19.3.609-620(2021).

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

Kostrubiec, J. (2013) Kontrola administracji publicznej, In: Karpiuk, M. & Kowalski, J. (eds.) *Administracja publiczna i prawo administracyjne w zarysie* (Iuris: Warszawa-Poznań), pp. 329-364.

Nowikowska, M. (2021) Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa, *Cybersecurity and Law*, 1, pp. 77-103.

Polinceusz, M. (2013) Nadzór nad administracją publiczną, In: Karpiuk, M. & Kowalski, J. (eds.) *Administracja publiczna i prawo administracyjne w zarysie* (Iuris: Warszawa-Poznań), pp. 311-327.

Procedural Provisions in the Convention on Cybercrime

FILIP RADONIEWICZ

Abstract The objective of this study is to analyse the solutions provided in the Council of Europe Convention on Cybercrime (ETS No. 185) of 23 November 2001 with regard to criminal procedures concerning the obtaining and preservation of evidence in the form of computer data, i.e. preservation of data (Articles 16 and 17), and four measures aimed at data collection (production orders – Article 18, search and seizure of stored computer data -– Article 19, real-time collection of traffic data – Article 20, and interception of content data – Article 21). The investigation of this subject-matter is preceded by an introductory part in which the key notions defined in the Convention on Cybercrime – namely computer data, computer system, service provider and traffic data – are discussed.

Keywords: • cybercrime • online search • on-line operational activities • hacking • interception of content data

CORRESPONDENCE ADDRESS: Filip Radoniewicz, Ph.D., War Studies University, Department of Cyber Security Law and New Technologies, Institute of Law, Centre for Cybersecurity Studies, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, e-mail: filip.radoniewicz@radoniewicz.eu, ORCID: 0000-0002-7917-4059.

https://doi.org/10.4335/2022.1.12 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The Convention on Cybercrime (the Council of Europe Convention on Cybercrime (ETS No. 185) of 23 November 2001) is the first international treaty that deals with combating crimes committed with the use of the Internet and computer networks.

Representatives of most Member States of the Council of Europe (including Poland) and, in the capacity of observers, delegates from the USA, Japan and Canada, representatives of EU institutions and independent experts took part in the works on the Convention, which took over four years to be completed. The objective of the Convention on Cybercrime was to create a legal framework for prosecuting crimes. Numerous innovative solutions were proposed in the Convention (innovative at the time – we should bear in mind that it was being drafted at the end of the last century). The list of offences was extended in relation to previous international documents (*Computer-Related Crime. Analysis of legal policy in the OECD Area*, OECD, ICCP Series No. 10, Paris 1986; *Recommendation No. R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*, Council of Europe, Publishing and Documentation Service, Strasbourg 1990). They include, i.a., illegal access, illegal interception, data interference, system interference, offences related to hacking tools – misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights). It also includes provisions concerning the penal liability related to individual stages of an offence (attempt), the forms of accessory liability (aiding and abetting), and corporate liability (this term is understood also as the liability of non-corporate organisational units). The Convention also sets out a number of procedural solutions, such as the preservation of data, search and seizure of stored computer data, etc. These were included in Section 2 of the Convention (Procedural law). They should, first and foremost, be applied to proceedings concerning "conventional" offences (i.e. offences established in accordance with Articles 2 through 11 of the Convention). In addition, they should be applied in relation to all other offences committed by means of a computer system, and the collection of evidence in electronic form in the course of criminal proceedings concerning other offences (Radoniewicz, 2016: 162-165).

2 Explanation of key terms

Before the provisions stipulated in Section 2 of the Convention are discussed, it is necessary to explicate the most important terms, i.e. "computer system", "computer data", "service provider" and "traffic data".

In the light of Article 1(a) of the Convention, a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

According to the Explanatory Report (*Explanatory Report to Convention on Cybercrime*

– a commentary to the Convention prepared by its authors, Points 23 and 24), a "computer system" is a device consisting of hardware and software. "Hardware" may include input, output and storage facilities. A 'computer program' is a set of instructions that can be executed by the computer system to achieve the intended result. A "computer system" usually consists of different devices. A "central processing unit" is the indispensible component. Other elements are "optional" and include "peripherals" (devices that perform certain specific functions in interaction with the processing unit, such as a video screen, printer, DVD reader/writer or other storage devices, etc.). In the light of the Convention on Cybercrime, computer systems include mobile phones, decoders and, most of all, a device which is commonly understood as a stand-alone "personal computer" (PC), i.e. a single host. Furthermore, two or more independent interconnected computer systems (i.e. able to communicate computer data) comprise a "network". The connections through which data is transmitted may be earthbound (e.g., wire or cable) and/or wireless (e.g., radio). A network may have a different geographical reach – from small "local area networks" (LANs) – composed of several computers, to networks spanning a large area ("wide area networks" – WANs). Computer systems may be connected to the network as endpoints (single hosts, decoders, phones, etc.) or as a means to assist in the data transfer process, such as routers or servers. The prerequisite for considering a given structure a network is the exchange of data over the network.

"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

As per Article 1(c) of the Convention, the term "service provider" is understood as 1) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and 2) any other entity that processes or stores computer data on behalf of such communication service or users of such service.

In general, the term "service provider" encompasses two categories of entities: "content providers", i.e. entities providing access to their own services (content) (e.g. web portal operators), and entities intermediating in the access to services – "intermediary service providers", broken down into "access providers" and "service providers", namely entities which transmit, store and provide access to information on the Internet. In some cases the same entity performs both functions, e.g. a web portal operator may at the same time post its own content (thus being a content provider) and render services to other entities, e.g. a hosting service (storage of data provided by third parties – clients). This usually consists in providing access to own servers (or, for instance, virtual digital platforms). It might include, for example, the maintenance of a client's website on a server, in which event, the service provider concerned assumes the role of an intermediary service provider. This distinction is significant from the legal point of view, due to the exclusion of liability in the event of rendering certain services by entities belonging to the last group (i.e. intermediary service provider offering the aforementioned hosting, mere conduit and caching (temporary and automated data storage in order to accelerate further access to it

– e.g. downloading the most popular websites among network users to the servers of a local area network to facilitate fast access to them).

Based on the definition provided in Article 1(c), it can be inferred that, for the purpose of the Convention on Cybercrime, the term 'service providers' refers only to the group of intermediary service providers. According to the definition, they encompass public or private entities which provide the users of its services the ability to communicate by means of a computer system, or other entities that process or store computer data on behalf of such communication service or users of such service (which means that they have mere conduit, hosting or caching in their service portfolio).

Under Article 1(d) of the Convention, "traffic data" is defined as any computer data relating to a communication by means of a computer system, generated by a computer system (e.g. a mobile phone, a computer, but also router or server, as points on the data transfer route) that formed a part in the chain of communication, indicating the communication's origin (a place where data transfer was initiated, expressed as, most of all, an IP address, optionally a phone number, or a similar identification of a communications facility to which a service provider renders services), destination (the identification data of a communications facility to which communications are transmitted is the same as that of the communications facility being a location where data transfer was initiated), route, time, date, size, duration, or type of underlying service (e.g. file transfer, or electronic mail). Traffic data can assume a dynamic form, i.e. data on transmission (data included in packet headers) and static form, such as system logs stored in firewalls, routers or servers (including information about any events taking place in the networks, including the details of participating entities). E-mail addresses and IP addresses are undoubtedly traffic data.

Certain doubts may arise when qualifying URL addresses or search criteria entered in a search engine. On the one hand, it is a set of simple instructions in a binary code, allowing users to obtain information from the web. In this context, they have the features of traffic data. On the other hand, they constitute a form of communication, because they indicate what a given user has in mind by entering a URL address or a phrase in a search engine. Similar issues can be observed as regards HTTP requests that may include such information as user's e-mail address, recently visited websites or search criteria (Clough, 2013: 153-154).

3 Conditions and safeguards

In Article 15 of the Convention, emphasis was placed on the protection of human rights. Pursuant to this provision, the establishment, implementation and application of the powers and procedures provided for in the Convention are subject to conditions and safeguards provided for under the domestic law of each Party, which should ensure the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the

Protection of Human Rights and Fundamental Freedoms (ECHR), the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments. It was also stressed that the adopted measures must incorporate the principle of proportionality, and such conditions and safeguards should, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party is obliged to consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties. Since the Convention is to be applied by states having different legal systems, it is not possible to define the conditions and safeguards applicable for each power and procedure provided for in its provisions. Therefore, certain common standards and minimum safeguards to be observed by Parties to the Convention have been indicated. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments, i.e. primarily the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols (Explanatory Report, Point 145).

4 Procedural provisions

The Convention provides for five new measures – one aimed at the preservation of data (Articles 16 and 17), and four aimed at data collection (production order – Article 18, search and seizure of stored computer data – Article 19, real-time collection of traffic data – Article 20, and interception of content data – Article 21).

The first of the instruments laid down in the Convention involves the granting of powers to competent law enforcement authorities of the Parties to order network administrators, or to similarly obtain, the expeditious preservation of specified computer data, including traffic data that has been stored by means of a computer system, and has probative value. This measure may be applied, in particular, where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

This construct should not be confused with data retention – which is limited to traffic data and includes the data of all entities operating in the network. It involves the retention by providers of publicly available electronic communications services or of a public communications network of the so-called “transfer data” (traffic and location data, and the related data necessary to identify the subscriber or registered user) generated or processed by such service providers, in order to ensure their availability for the purposes of investigation, detection and prosecution of criminal offences. As regards EU law, the obligation to retain data for a period of not less than six months and not more than two years from the date of the communication was imposed under Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic

communications services or of public communications networks and amending Directive 2002/58/EC (OJ EU 2006 L 105/54). It was rendered invalid as a result of the Judgement of the Court of Justice of 8 April 2014 (Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications et al., ECLI:EU:C:2014:238).

The preservation of data provided for in the Convention refers to specific data regardless of data type.

The preservation order should impose an obligation on the person in possession of (or controlling) computer data to preserve and maintain the integrity of specified stored computer data in that person's possession or control for as long as necessary, but no longer than ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. There should also be a possibility to oblige the custodian or other person required to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law (Article 16(3)).

As regards traffic data to be preserved under Article 16, in Article 17, it is stipulated that Parties are obliged to ensure that the expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication, and ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the authority to identify the service providers and the path through which the communication was transmitted.

Due to the significant controversies between state governments in relation to the issues of cross-border evidence collection, the Convention does not impose any specific solutions in this respect, instead only encouraging states to cooperate on this matter. Accordingly, the cross-border access to evidence will be as deemed appropriate by a given state, in line with the recommendations of the Convention. It is an open issue whether solutions will be harmonised. However, the Convention requires the adoption of certain "minimum procedures" (see Article 23) (Weismann 2011: 273).

The next legal construct provided for in the Convention is the "production order" described in Article 18. It may be addressed both to a person in the territory of the issuing party, and to a service provider offering its services in the territory of the Party. In the former case, it entails an obligation of the person indicated in the order to submit specified computer data in that person's possession or control, which is stored on a computer system or a computer-data storage medium, and as regards the latter case, an obligation to "submit subscriber information" relating to such services in that service provider's possession or control. As per Article 18(3), "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, and by which can be established: 1) the type of communication service used, the technical

provisions taken thereto and the period of service; 2) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; 3) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

Article 19(1) provides for a measure that involves empowering competent law enforcement authorities of a Party to search a computer system or part of it and computer data stored therein, and a computer-data storage medium in which computer data may be stored, or "similarly access" a computer system or part of it and computer data stored therein, and a computer-data storage medium in which computer data may be stored in its territory.

Article 19(2) of the Convention provides an "invasive" form of search, i.e. extended search. The provision allows law enforcement authorities to extend the scope of "search operations" (e.g. to search or similarly access computer data, as provided for in Article 19(1a)) to include the resources stored in another computer system or its part, accessible from or available to the initial system, if they have grounds to believe that the data sought is stored in another computer system or part of it. The other computer system or its part must be located in the territory of the state concerned. The convention does not define the procedure for extending the search. This is left to domestic law. The authors of the Convention give several examples of possible solutions: 1) empowering the judicial or other authority which authorised the search of a specific computer system ("initial" computer system) in a specified network (mainly LAN) to authorise the extension of the search or similar access to a connected system ("secondary or further computer system") if there are grounds to believe (to the degree required by national law and human rights safeguards – e.g. high probability verging on certainty) that the connected computer system may contain the specific data that is being sought in proceedings under which a relevant decision has been issued; 2) empowering the investigative authorities to extend an authorised search or similar access of a specific computer system to a connected computer system where there are similar grounds to believe that the specific data being sought, relevant to the proceedings being conducted, is stored in the other computer system; 3) or exercising search or similar access powers at several locations simultaneously (i.e. both in the initial and secondary systems, which means that it is not precisely an extended search, taking into account that the secondary system is not accessed through the initial system in this case) in a coordinated and expeditious manner (so-called "simultaneous search").

In all cases, the data to be searched must be lawfully accessible from or available to the initial computer system (Explanatory Report, Points 193-195).

It is worth stressing that the extended search constitutes a significant interference in the privacy of computer system users, as there is no possibility to control the search operations, and law enforcement authorities gain wide access to data during the search,

whereas at the same time the rights of persons affected by such actions are not properly secured (it is worth remembering that these are often random computer systems – for example, systems connected to the same local area network).

For that reason, search extension was one of the several solutions which were most criticised by non-governmental organisations during the works on the Convention (in addition to criminalising activities concerning the so-called "hacking tools" – Article 6 of the Convention).

Therefore, the parties to the Convention have been obliged to establish conditions and safeguards which should provide for the adequate protection of human rights and liberties (the aforementioned Article 15).

I believe that, in line with the principle of proportionality and subsidiarity, it would be advisable to include a provision stipulating that a search may only be extended where it is not possible to otherwise obtain the data sought, and in the event where there is a high probability that the data is stored in a connected computer system, while the application of the measure should be limited to matters related to the most serious prohibited acts provided for by law.

Paragraph 3 sets out the obligation to empower the competent authorities of a Party to seize or similarly secure computer data accessed as a result of search, including the power to: 1) seize or similarly secure a computer system or part of it or a computer-data storage medium; 2) make and retain a copy of those computer data; 3) maintain the integrity of the relevant stored computer data; 4) render inaccessible or remove those computer data in the accessed computer system.

According to the authors of the Convention, it is necessary to empower its competent law enforcement authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as reasonable, the necessary information to enable the undertaking of the relevant measures (Article 19(4)).

Pursuant to Article 20(1), a measure entailing the real-time collection of traffic data was introduced. The Convention provides for its two variants, including the collection or record of data through the application of technical means independently by a competent authority, or through, or with the assistance of, service providers, as the Parties may compel a service provider to collect or record traffic data through the application of its own technical means or to co-operate and assist the competent authorities in these operations. The two variants are not alternatives – each Party must ensure that both measures can be carried out. According to Point 223 of the Explanatory Report, such solution is necessary in case a service provider does not have the technical ability to assume the collection or recording of traffic data. Furthermore, in the event of some local area networks (LANs), where no service provider may be involved, the only way for

collection or recording to be carried out would be for the law enforcement authorities to do it themselves. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures in question, it may limit itself to other measures, such as only relying on the operations of service providers (Article 20(2)).

The discussed provision at the same time limits the adoption of the measures by a Party to criminal proceedings in specific cases, and to traffic data associated with specified communications "in its territory."

Each Party should adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in the discussed Article (Article 20(3)).

As regards the interception of content data (computer surveillance), it is assumed that this investigative measure must be restricted to a range of serious offences. The initiative to compile a list of such offences is left to the Parties.

The measure may be applied only in the course of criminal proceedings, as it entails the collection of content data, in real-time, of specified communications in its territory transmitted by means of a computer system. Similarly to traffic data, the Convention provides for two possible variants of such measures – the collection and recording of content data by law enforcement authorities, and "the employment" of service providers to perform the activities, so that within their existing technical capability, they collect or record content data through the application of technical means on the territory of that Party, or co-operate and assist the competent authorities in the collection or recording of content data. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1(a) (collection and recording of data by law enforcement bodies), such Party may limit the measures to relying on the operations of service providers only.

Of course, similarly to collecting and recording traffic data, each Party should adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in the discussed Article (Article 21(3)).

Each Party may reserve the right to apply the measures stipulated in Article 20 solely to criminal offences or categories of offences specified in the reservation, provided that the scope of such offences or categories is not more restricted than the scope of offences to which it applies the interception measures referred to in Article 21. Each Party should consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20 (Article 14(3)(a)). Where a Party, due to limitations in its legislation in force is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system is being operated for the benefit of a closed group of users, and does not employ

public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications.

At the same, it has been stressed that each Party should consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20 (Article 14(3)(b)).

To conclude, it is worth mentioning one more important issue – the nature of traffic data and the degree of its protection. As noted above, the data includes information on the events in the network and details of participating entities. Therefore, they have significant probative value. At the same time, the data can say a lot about network users (whom a given person has contacted, which websites he/she visited, what services he/she uses ...). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures, pursuant to Articles 14 and 15 (Explanatory Report, Point 227). It should be noted that the European Court of Human Rights (ECtHR) found that the use of traffic data constituted interference in the right to respect for private life, within the meaning of Article 8 of the ECHR. In the Judgement in the Malone v. the United Kingdom case (ECtHR Judgement of 2 August 1984, Application No. 8691/79), the Court found that the so called "metering" (recording phone calls made from a given device by registering the numbers dialled and the time and duration of each call), which is a standard activity made by telecommunications service suppliers, per se cannot be considered as interference in the right to privacy. However, the release of the information obtained this way without the consent of the subscriber amounts to the interference with a right guaranteed by Article 8 ECHR. In the Court's view, this stems from the fact that the metering records contain information that is an integral element in the communications made by telephone. In a ruling made in the Copland case (ECtHR Judgement of 3 April 2007 in the Copland v. the United Kingdom case, application No. 62617/00), the Court stressed that the data related to e-mail and Internet usage (i.e. traffic data) were subject to protection equivalent to that of telephone conversations.

5 Conclusions

It is a truism to say that international cooperation is of key significance in combating offences committed by means of computer networks. Telecommunications networks span the entire globe. The perpetrators' conduct can simultaneously affect numerous countries located in distant parts of the world. In addition to close cooperation between law enforcement authorities, as one of the formal conditions of such collaboration (due to the principle of dual criminality), it is important to ensure the criminalisation of computer crimes in the greatest possible number of states, reaching a situation where there are no so-called "hacker havens", which are the countries in which their operations are not prosecuted, and to introduce legal measures allowing the conduct of criminal proceedings

in cybercrime matters in the legislations of such states, such measures being "on-line" operational activities discussed in the present study.

Currently, the only international agreement addressing measures against computer crime is the Convention on Cybercrime. This paper discussed the procedural solutions proposed in the Convention. As of time this paper was written, they should have been adopted in several dozen countries that have ratified the Convention. Some of its unquestionable advantages include the open-ended nature of the Convention – it may be acceded by states that are not members of the Council of Europe, and the provisions of optional clauses. They allow the adoption of the Convention on Cybercrime with the exception of certain provisions, thanks to which the state parties implementing the Convention to their domestic laws may reconcile it with their own legal tradition and culture, and the legal regulations in force. Given the above, nearly all Member States of the Council of Europe signed the Convention on Cybercrime by 17 September 2021 (46 countries to be exact, as only Russia has not signed the Convention), and 45 states ratified the document (apart from Russia, which is obvious, Ireland has not ratified the Convention yet). The Convention has also been signed by four non-European states (Canada, Japan, the United States, the Republic of South Africa; and ratified by three of these countries, except the RSA), while further 17 countries (including Australia, Dominican Republic, Israel, Panama) acceded to it. In total, the Convention was ratified by 66 states. As a side note, it should be mentioned that numerous countries that had not signed the Convention decided to use its provisions to draft their own domestic laws. They include Botswana, Egypt, the Philippines, and Pakistan (Brunst, Gecrke, 2009: 53).

References:

Clough, J. (2013) *Principles of Cybercrime* (Cambridge: University Press).
Brunst, P.W. & Gecrke, M. (2009) *Praxishandbuch Internetstrafrecht* (Stuttgart: Kohlhammer).
Radoniewicz, F. (2016) *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym* (Warszawa: Wolters Kluwer).
Weismann, M.F. (2011) International cybercrime: Recent developments in the law, In: Clifford, R.D. (ed.) *Cybercrime: The Investigation, Prosecution and Defense of a Computer-related Crime* (Carolina: Academic Press), pp. 257-294.

Management in Cyberspace: From Firewall to Zero Trust

WOJCIECH PIZŁO

Abstract Households, enterprises, as well as the entire sphere of public services, are undergoing intense digitization. We are learning to use information and communication tools at work to a greater extent than before and enterprises are increasingly using new technologies to improve management in many spheres. The aim of this research is to identify changes in the approach to management in cyberspace that are mediated by information technologies. This paper presents the key issues pertaining to the definition of cyberspace, defines the characteristics of cyberspace management and the framework regulating its functioning – international and national legislation. Additionally, it discusses the principles of risk management in cyberspace, including the core principles of cybersecurity, best practices of regulators, as well as the approach to security known as Zero Trust.

Keywords: • cyberspace management • zero trust • digital security • cyberspace regulations

CORRESPONDENCE ADDRESS: Wojciech Pizło, BEng, Ph.D., Dr. Habil., University Professor, Warsaw University of Life Sciences (SGGW), Institute of Management, Nowoursynowska (Street) 166, 02-787 Warszawa, Poland, e-mail: wojciech_pizlo@sggw.edu.pl, ORCID:0000-0002-5212-0990.

https://doi.org/10.4335/2022.1.13 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Remote work has become an essential part of many areas of the economy, in particular public services such as medical care and education. The scope of computerization of societies and the global economy has expanded considerably. Consequently, the increased dependence of citizens and businesses on the provision of digital services and the related availability of technical infrastructure can be observed. Management in the sphere of cyberspace is related to property rights, IT resources, the availability of technical infrastructure as well as the capabilities of people operating in the digital space.

Due to the implementation of information and communication technologies in various spheres of life, enterprises are subject to intense changes. Research shows that in organizations with a hierarchical structure, the flow of information is limited (Jarvempaa & Tanriverdi 2003: 403-412). The universal access to IT tools results in flattening of the organizational structures and change in power dynamics (networking of power) in organizations which often gains an informal dimension. Organizations, even small and medium-sized enterprises, create networks of relationships that extend beyond national borders. For this purpose, they use modern technologies to build groups of customers, suppliers and business partners. Business networks, modern IT tools, databases, and above all, creative people constitute the basis for creating new organizational solutions and new management methods characterized by high degree of flexibility and efficiency (Snellman, 2014: 1251-1261). The emergence and dynamic development of social and market cyberspace produce changes in social relations and transform the management methods (Pizło, Parzonko, 2022: 61-79), the organizational structure of enterprises, and stimulate the creation of organizations, (not only enterprises), which are designed from the very beginning as virtual. The literature indicates that the main factors mediating new management solutions are the construction of open virtual organizations and the lack of administratively limited access to selected innovative technologies (Gassmann, 2006: 223-228). The currently used knowledge management support tools (Le-Nguyen, Dyerson, Harindranath, 2018: 1117-1133) include: document management systems (Sun, Lei, Cao, Zhong, Wei, Li, Yang, 2020), Web 2.0 (Orenga-Roglá, Chalmeta, 2019: 195-213), supporting the development of innovation (Schmidt, von der Oelsnitz, 2020: 9-21) and team work, as well as corporate portals and decision support systems.

The aim of this research is to identify changes in the approach to management in cyberspace mediated by information technologies. The paper addresses the following research questions: 1) How are the issues of cyberspace and cybersecurity perceived in the literature?; 2) What are the characteristics of cyberspace management, taking into account the zero trust approach?

The research method was desk based analysis of literature. The data sources included the selected publications from Elsevier and Researchgate databases.

2 Definition of cyberspace

The term "cyber" used in the literature usually refers to two elements, namely, the virtual reality and the interconnected electronic communication networks. In the case of virtual reality, the emphasis is put on the intangible nature of the maintained relationships; in the second approach, the concept of "cyberspace" is synonymous with the Internet. This concept is broader because it covers any network connecting information systems, including local area networks (LAN), i.e. a local computer network that connects selected areas, e.g. laboratories, offices, or entire enterprises and wide area network (WAN), which is a computer network extending beyond urban agglomerations, the country even the continent. Cyberspace is defined as "(...) a collection of interconnected computerized networks, including services, computer systems, embedded processors and controllers, as well as information in storage or transit" (Refsdal, Solhaug, & Stølen, 2015), and also as "global domain within the information environment, consisting of an interdependent network of information systems infrastructure, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" (NIST, 2020). The concept of cyberspace in military terminology refers to (DOD 2021) infrastructure and systems supporting it. In this approach, cyberspace is defined as "the global domain within the information environment consisting of interdependent networks of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DOD 2021: 55). The cyberspace security is defined as "actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation". The concepts of cyberspace are based on several important elements, that is: 1) human perception penetrating the world of information, both posted and created on the network; 2) range of impact; 3) virtual reality.

3 Management in cyberspace

An important aspect of cyberspace realm is cyberspace management, which strives to organize the processes taking place there. Management in cyberspace is determined by the framework of international law and national regulations, as well as the capabilities to manage the organization's resources in cyberspace. The purpose of this activity is, on the one hand, to maximize the benefits of using new technologies and, at the same time, to minimize the risk of their negative effects. The activities of enterprises in business cyberspace have been carried out for several dozen years. The wide spread of new technologies has made security in the digital space one of the key sources of threats. Cybersecurity covers a wide spectrum of challenges e.g. ensuring the free use of critical infrastructure, influencing civic participation, such as elections in democratic countries, as well as preventing the loss of key data by strategically important enterprises and organizations. The threat comes not only from hostile countries, but also from competing

enterprises as well as criminal and terrorist organizations. One of the first studies on cybersecurity referred to: the design of cyberspace intrusion detection systems requiring the fusion of data from myriad heterogeneous distributed network sensors (Bass 2000: 99-105), as well as insurance covering the potential loss of important information as a result of cyber-attacks (Biener , Eling, Wirfs 2015: 131-158). In the inclusive approach, "cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". (Craigen, Diakun-Thibault, Purse, 2014). The intention of the authors of this definition was to emphasize the interdisciplinary nature of the concept of cybersecurity and thus change the approach of scientists, financing agencies and the organizations themselves to the challenges related to cybersecurity. This approach shifts the focus from the technical point of view to the interdisciplinary perspective, supporting inclusiveness, as well as through the relationship with other functional areas of cyberspace and pointing to the issues of access to resources and property rights. The issue of organizations' willingness to invest in cybersecurity is thoroughly analyzed in research by Wessels, van den Brink, Verburgh, et al. (2021) which provides a typology of incentives for cybersecurity investments. Research on cybersecurity is often based on the Global Cybersecurity Index, which measures the commitment of countries to cybersecurity at a global level to raise awareness of the importance and different dimensions of the issue. It indicates that most governments have developed national cybersecurity defense strategies to combat the cybersecurity risks (Fadia, Nayfeh, Noble, 2020: 2), because an increasing group of citizens, enterprises and public institutions managing critical infrastructure is exposed to cyber attacks.

The literature points to the role of cybersecurity and the associated risks related to the economic situation of enterprises (Yang, Lau, Gan 2020: 167-183), and also emphasizes the relationship between the competitive strength of individual enterprises and the trust of various entities, including investors, in the information security management. People create communities by working, having fun and spending time together. Every time they do so, they benefit from trust. In online communication people are unable to verify who they are interacting with. Online communication adds new dimensions to trust (Marsh, Atele-Williams, Basu, Dwyer, Lewis, Miller-Bakewell, Pitt, 2020). The role of the state is to build trust and security in cyberspace. The pandemic has indicated a different approach to understanding macroeconomic principles of operation in the field of cyber security (Global Cybersecurity Index 2021). Trust is important in a society and digital economy, because the main trust-encouraging features on the Internet is transparent and reliable data, but most of all, what is emphasized in the literature, is the "need to democratize big data, and not let it be the preserve of corporate, scientific, or political elites" (Marsh, et al 2020). The essence is the responsible and ethical use of big data instead of using it for business purposes (corporate power) or political purposes, especially when it comes to lowering the rank of democracy (power of political parties) or in scientific circles (power of knowledge).

The core principle of enterprises' activities in cyberspace is the creation of an individual model of reacting to potential malicious incidents. Concern for maintaining a high level of security and minimizing cyber risk is important in the long-term perspective. It is confirmed (Ferens, 2021) that information on cyber threats is important enough to be consolidated and standardized. Cyberspace is built by individual network elements, but even when one network is secure; it is not known how it will behave in an interaction with other network elements of other entities. Relationships between several elements can lead to unpredictable instability (Helbing, 2013: 51-59).

4 Risk management in cyberspace

Risk management in the case of organizations operating in cyberspace consists of: 1) identification of goals; 2) risk determination; 3) assessment of the probability of cyber incident occurrence; 4) avoiding and mitigating the negative effects of a cyber attack; 5) continual monitoring of threats. The implementation of the indicated elements of cyber risk management depends on the IT department's ability to cooperate with other parts of the organization. It is indicated in the literature that enterprises holding the position of the head of information security or a similar position bear lower costs related to cyber attacks. In the case of some countries, having a digital security certificate opens the public procurement market for the company. This takes place in Japan and the countries of the European Union.

5 Cybersecurity in different economic systems

The literature indicates that (Biener, Eling, Wirfs 2015: 131-158) cybersecurity is a public good and the market provides an insufficient level of cybersecurity, therefore government interventions such as subsidies for technological support preventing cyber attacks or compulsory cybersecurity insurance may be considered. Governments, at least a considerable number of them, focus their efforts on preventing and cyber attacks, mitigating their effects and protecting their citizens, businesses and critical infrastructure. The main regulators, which are states and institutions of international law, have the possibility to directly increase cybersecurity through appropriate legislation, as well as, by acting indirectly to stimulate the desired behavior of both organizations and individuals in the field of cybersecurity.

In economics, two different approaches to market regulation are differentiated. The first approach is the command-and-control regulation consisting in an arbitrary determination of the rules regulating the market. The second approach involves regulation through economic incentives or automatic regulation or self-regulation developed by a given community. In the case of "motivated regulations" defined through the prism of the applied rewards and penalties, their aim is to achieve the desired results, while maintaining a certain decision-making autonomy. Giving freedom to the actors in the market does not mean that the regulator's decision is the only single factor, (even if it is one of the stronger ones), but it is always one of the many stimuli that coexist in the

structure of stimuli. Another approach to "motivated regulation" is the perception of markets through the prism of people's inclination to build social bonds, spontaneous knowledge sharing (Smith, 2013, XXXVI, 50-57), which is the foundation for creating new markets. In this case, the knowledge and skills of the community constitute the basis for spontaneously arising rules that often create a sophisticated system of using shared resources by community members (Ostrom, 2013).

An important element of building a rational framework of regulations relating to cyberspace is the use of the provisions of the Budapest Convention (Convention on Cybercrime, 2001) ratified by over 60 countries and the EU Directive 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. The Budapest Convention recommends the adoption of substantive and procedural regulations. The substantive regulations define different types of cybercrime, including copyright infringement, computer-related fraud, data and systems interference and child pornography. In turn, the procedural regulations provide the law tools to investigate cybercrime and secure electronic evidence in relation to any crime. Due to technological progress, the rules of enacting cyberspace law should be modified in order to keep up with the innovativeness of the market. The element that binds the cybersecurity system is the observation of both the development of technology and social attitudes towards potential threats.

When building national institutional structures dealing with cybersecurity, it is necessary to consider the following questions (Fadia, Nayfeh, Noble, 2020): 1) Should the agency reside within a defense and intelligence entity or within a civilian body? 2) What level in the government does the agency report to? 3) What is the scope of the agency’s control and oversight (for example, does it focus only on critical infrastructure or also on citizens and small and midsize businesses)? The questions should be treated rhetorically, as they refer to the choices that reflect the "philosophy" of internal policy, the development of cyber infrastructure and aspirations in the field of cybersecurity of an individual country.

Cyber risk is a derivative of the regulatory approach to the issue of how to ensure security and related to the behavior of network users as a result of which identity theft (loss) and disclosure of confidential, most often personal, information occurs. The probability of a threat related to interference in the managed cyberspace of the enterprise is referred to as cyber risk (Eling, Schnell, 2021). Knowledge of the market and threats in cyberspace minimizes the likelihood of its negative effects, and also contributes to easier modeling and management of this type of threat.

The simplest division of cyber risk is the indication of threats caused by independent natural factors causing mechanical damage to IT infrastructure and man-made threats (intentional and unintentional). The susceptibility of enterprises to cybercrime threats may be determined by the specific features of the organization that minimize the threat of a cyber attack. These specific features include: technology that the company has at its

disposal, processes as well as knowledge and IT skills of employees. Threats of cyber attacks result from the widespread use of IT tools both in public administration and private enterprises. The changing area of cyber threats makes it necessary to observe a wide and interdisciplinary spectrum of issues.

The research results indicate that (Naseer, Maynard, Desouza, 2021) the ability to quickly detect and effectively respond to cyber attacks is an important element of the efficient operation of any organization (Ahmad, Desouza, Maynard, Naseer, Baskerville, 2020: 939-953). The diagnosis of the threat, and in particular the response to incidents, i.e. incident detection, diagnosis of the areas of interference and its elimination, as well as restoration of the original state and elimination of the possibility of similar interference in the future, is the essence of rational counteracting cyber threats. The principal element of counteracting cyber attacks is the constant operation of an interdisciplinary team, whose task is to observe the information system, assess events and report on cybersecurity in an enterprise described as agile – capable of rapid reacting to unexpected challenges. An important factor of success (preventing interference) is the time that elapses from the detection of a cyber attack to the system recovery. The speed of this reaction is called agility and is important because the probability of a negative impact on the organization increases with time distance from the detection of the incident. The essence of counteracting cyber threats is collecting, storing and analyzing all data related to the incident.

6 Best practicies of cybermarket regulators

The McKinsey & Company report (2020) compared cyber security strategies in 11 countries that are best organized in this respect. The research has identified five components of a successful cybersecurity strategy. Firstly, it is the existence of a dedicated national cybersecurity agency (NCA), the aim of which is macroeconomic and macrosocial cybersecurity, secondly, a national critical infrastructure protection program, thirdly, a national incident response and recovery plan, fourthly, clearly defined legal regulations concerning cybercrime, and lastly, ensuring an efficient cybersecurity ecosystem. The recommendations of the report, summarizing good practices of best-in-class countries, include: 1) the need to establish a national cybersecurity agency responsible for defining and driving the cybersecurity agenda of the entire country; 2) the need to develop a cohesive national cybersecurity strategy to protect the critical infrastructure of the country; 3) define a wide range of actions in response to cyber incidents, including in particular the definition of cybersecurity standards; 4) improving the cyber awareness of citizens; 5) developing the cybersecurity capabilities of professionals.

A priority recommendation for public authorities is to eliminate the risk of a cyber attack on the national critical infrastructure which may lead to disruptions in other sectors of public life. Critical infrastructure is an attractive target for both hostile state actors and hostile organizations seeking publicity. Effective cyber attacks have a negative impact on

the economy, society and business confidence, and undermine national defense capabilities. The best cybersecurity programs targeting critical infrastructure focus on selecting critical sectors and assets to be specially protected. The choice of critical areas depends on the way in which the rulers define the role of individual sectors of the economy, well-being of the society, and national security of the country. The experience of countries with the best system of counteracting cyber attacks indicates the need to respond to incidents even when their losses are relatively small and recovery activities are ongoing (Fadia, Nayfeh, Noble, 2020: 2). The essence of counteracting is not only to prevent negative events, but if they occur, learn about their mechanism and mitigate their negative effects.

The McKinsey report (Fadia, Nayfeh, Noble, 2020: 2) defines actions needed to counteract cyber attacks, i.e. procedures for reporting observed incidents (cyber attacks) by citizens and enterprises. The best results were achieved in those countries where it was clearly defined to whom cyber incidents could be reported by institutions, citizens and enterprises. It was recommended (Fadia, Nayfeh, Noble, 2020: 2) to build a centralized repository where all data on cyber threats and cyber attacks will be collected. In addition to passively recording all reported cybercrimes, central institutions must actively monitor the Internet for cyber threats. The traditional national security intelligence to monitor threats should be combined with other channels like a platform collecting confidential information from the private sector (Great Britain - Cyber Security Information Sharing Partnership). This platform allows for quick and confidential sharing of information about threats. An important element of active protection against cyber attacks is automated manner of counteracting cyber threats (National Cyber Security Centre in Great Britain). When malicious content is detected on a website, the system blocks this content nationwide and works with the hosting company to remove it. Each cyber incident should be classified based on its level of threat in relation to e.g. critical infrastructure, national security or other socially and economically important criteria, as well as the type of victim and the expected interdependence of cyber threats, because a cyber attack on a "small" entity may be a preparation to attack an important public institution. The introduction of standardization of incidents organizes risk management in public cyberspace, allowing for a rational and orderly minimization of the risk of a cyber attack. Determining the threat level together with the "severity assessment matrix" is part of a well-developed mobilization plan that enumerates public entities that should respond to cyber incidents of varied severity. A local incident, such as a break-in into a small enterprise, is the domain of the local police, supported by procedures and expert advice from a national cybersecurity agency. On the other hand, counteracting threats to critical infrastructure should be coordinated, among others, by the police, proper sector regulator, intelligence agencies, etc., where the coordinating entity is a national cybersecurity agency.

7 Zero trust security model

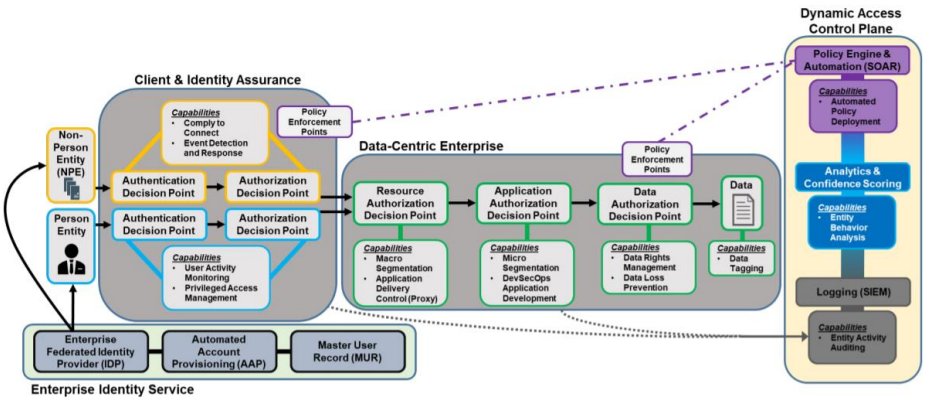
Contemporary organizations, when it comes to information systems, do not have easily identifiable borders. They rely on complex multifunctional systems supporting corporate offices, production departments, warehouses, sales and marketing departments including remotely working sales representatives, accounting and logistics. The complexity of such systems makes it difficult to protect them against cyber attacks (Department of Defense, 2021). One of the pioneers of the zero trust approach was. J. Kindervag (2010) who noticed that the dominant concept of categorizing network users into trusted and untrusted is not effective enough. The new approach, now known as zero tust, adopts the principle that no implicit trust is granted to any user or process. This approach assumes that the attacker is already present on the network. Therefore, an algorithm is used to grant access based on detailed requests. The following principles underlying the concept of zero trust (Kindervag, 2010) are indicated: 1) ensuring secure access to all resources regardless of location. This approach assumes that all network traffic is a potential threat until it is verified and secured; 2) adopting the strategy of the lowest privilege and strictly enforcing access controls. It is assumed that each user in the network must have limited – minimal, but sufficient for effective work - rights, with simultaneous strict (regulated) access to sensitive resources of the organization. Users who have access to the network are continuously monitored to determine if their activity does not deviate from the adopted security standards. The zero trust concept assumes that the network traffic is registered, verified and the response to unusual events is immediate.

The National Institute of Standards and Technology (NIST) pointed to the main factors that determine the choice of a zero-trust strategy by an organization (Rose, Borchert, Mitchell, Connelly, 2020). In the case of an enterprise, they may have a complex system serving the organization's network. The internal network may include: 1) a remote office with its own local infrastructure; 2) remote and/or mobile workers; 3) cloud services. Building security based on perimeters (firewalls) by such an organization is insufficient because after defeating the security, access to the organization's resources is unlimited (Rose, Borchert, Mitchell, Connelly, 2020).

The concept of zero trust in cybersecurity was developed at the Defense Information Systems Agency (DISA) and the US Department of Defense, where a strategy ensuring cybersecurity for enterprises referred to as "black core" was developed. Since 2004, the idea of "deperimeterization" has been promoted, which consisted in eliminating the implicit trust, which based, inter alia, on the location of the network, its static protection and static defense mechanisms in a large segment of the network (The Jericho Forum, 2007). The concept of "deperimeterization" has been changed, improved and called "zero trust". Today, the term "zero trust" is understood as a new cybersecurity paradigm that shifts defense from network-based perimeters to users, assets and resources. The zero trust strategy assumes that there is no basis for implicit trust. Trust cannot be completely based on the physical or network location, and on the ownership of assets, such as ownership of a business and its domain. Adopting a zero trust attitude in cybersecurity

requires designing a simpler and safer architecture of the company's IT system. While the classic approach to cybersecurity assumed "defense in depth", zero trust promotes a more secure, coordinated, seamless, transparent, and cost effective IT architecture. The core of zero trust is the principle of Continuous Diagnostics and Mitigation (CDM), related to external malicious interference harmful to the organization. The activities of the organization are aimed at limiting the access of persons and institutions to information resources and making them available only to authorized persons. Zero trust is a strategy that applies to the entire information architecture. The purpose of this approach is to prevent access to critical resources of the organization. The organization adopting this IT development strategy undertakes to secure, manage and monitor every device, user, application and network transaction occurring at the perimeter and/or within the network enclave (Department of Defense (DOD), 2021). In this approach, it is assumed that no entity, system, network or service operating outside or within the space used by the organization is secure. The organization and its structures must verify everything and everyone who tries to access their resources.

Figure 1: Zero trust security concept



Source: Department of Defense (DOD) Zero Trust Reference Architecture, ver. 1.0, (2021), Agency (DISA) and National Security Agency (NSA):12. https://dodcio.defense.gov (Access. 10 September 2021).

The adoption of the high-level zero trust operation concept implies the acceptance of such information architecture where non-person entity identity and user identity are tracked independently allowing for separate paths of validating confidence levels. Authentication and authorization activities are performed at defined points in the enterprise. In the enterprises where the zero trust concept is applied, the confidence level for individual devices and users is determined and the access level is adjusted to the current defined threats. Users and non-person entities have a confidence level assigned to them. In the case of an assessment that the level of threat to the organization is above the set threshold,

such an entity does not receive access to a given digital space. Both the access itself and the data are protected by the Data Loss Prevention System. Control of access to enterprise resources is related to the diagnosis of the risk level of both users and devices used by a given entity.

The zero trust architecture should include (Department of Defense, 2021): 1) Identity Provider - a system performing direct authentication 2) Automatic Account Provisioning – a system providing identity governance services such as user entitlement management, business role auditing and enforcement and account provisions and deprovisioning 3) Master User Record – a system reporting on the access of individual people and devices to the system and subsystems as well as to individual applications. In addition, MUR provides the identification of internal and external threats and the circumstances in which users are granted or denied access to the resources of the organization 4) Privileged Access Management - a system that secure, control, manage and monitor privileged access to critical assets. This includes administrative access of systems, applications and services.

Both private and public enterprises as well as numerous government agencies and non-profit organizations have embraced or are transitioning to a security strategy based on the principles of zero trust. There are several concepts regarding the zero trust approach in cybersecurity management in an organization. First, there is an assumption that there is no longer a trusted interface on our security devices; second, there is no longer a trusted network; and third, there are no longer trusted users (Kindervag, 2010: 2). In this approach, it is recommended to treat all network traffic as involving risk. At the same time, Kindervag notes that this concept does not imply that employees are untrustworthy; however, the concept of implicit trust should not be applied to network traffic and data. By not granting trust to the activities that take place in the network, we reduce the likelihood of abuse of procedures and inappropriate use of the network. The chance of detecting non-standard activities and, consequently, cybercrimes also increases.

8 Conclusions

In recent decades, management in the cyberspace sphere has been dominated by people professionally involved in building telecommunications and information systems. This environment has imposed a technology-focused perception of cyberspace, limiting it mainly to technological issues. Managerial approach to cyberspace and cybersecurity refers to the social dimension of the relationship between employees, as well as between a device and an employee. The dissemination of information technologies modifies the shape of an organization, as the flow of information has become widespread. The structures of many organizations are more flattened; power dynamics changes as it becomes more networked and often gains an informal dimension. The dynamic development of social and market cyberspace entails changes in social relations, and along with them, management methods are modified to adapt to new conditions. An important area of cyberspace is cyber management, which is a set of strategies undertaken

to effectively manage the information resources owned by organizations. The framework of management activity is determined, on the one hand, by the international law and national regulations, on the other hand, by individual capabilities of an organization to manage its digital resources.

The state plays an important role in shaping cybersecurity and market rules. In economics, and in particular in institutional economics, two basic concepts of regulating the market are recognized. The first regulatory technique is the command-and-control approach consisting in arbitrary determination of the market rules, where representatives of the political power take the floor and not the community affected by the regulation. The second approach to regulating the market is self-regulation developed by a given community. Giving the market actors the freedom to regulate it is often a simpler solution, and in most cases respected by the community. In the case of cyberspace, neither the knowledge nor capabilities of the community constitute sufficient competence to regulate the market. Therefore, it would be advisable to refer to the provisions of the Budapest Convention ratified by over 60 countries and the European Union Directive concerning measures for a high common level of security of network and information systems across the Union. In addition to legal regulations, an important area is the development of a cybersecurity strategy, involving the widest possible cooperation between specialized national cybersecurity agencies. Good practices of best-in-class countries show that it is necessary to establish a national cybersecurity agency, to develop strategies needed to reduce cyber threats, to define actions to be taken in response to cyber incidents, to improve citizens' cybersecurity awareness and to enhance the competences of cybersecurity professionals. An important recommendation that can be taken into account both in macro terms and for individual organizations is the implementation of zero trust strategy. It is based on the assumption that no user or network can be implicitly trusted and must always be verified. Zero trust concept represents a new cybersecurity paradigm that shifts defense from web-based perimeters to users (both non-person and person entities).

References:

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H. & Baskerville, R. L. (2020) How integration of cyber security management and incident response enables organizational learning, *Journal of the Association for Information Science and Technology*, 71, pp. 939-953, https://doi.org/10.1002/asi.24311.

Bass T. (2000) Intrusion detection systems and multisensor data fusion: Creating cyberspace situational awareness, *Communications of the ACM*, 43, pp. 99-105.

Biener C., Eling M., & Wirfs J.H. (2015) Insurability of cyber risk: An empirical analysis, *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40, pp. 131-158.

Convention on Cybercrime (Budapest, November 23, 2001), available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[0]} (August 18, 2021).

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining cybersecurity, *Technology Innovation Management Review*, 4, pp. 13-21, https://doi.org/10.22215/timreview835.

Creazza, A., Colicchia, C., Spiezia, S. & Dallari S. (2021) Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era, *Supply Chain Management*, Vol. ahead-of-print (No. ahead-of-print), https://doi.org/10.1108/SCM-02-2020-0073.

Department of Defense (DOD) Zero Trust Reference Architecture, ver. 1.0 (2021) Agency (DISA) and National Security Agency (NSA), available at: https://dodcio.defense.gov (August 18, 2021).

DOD Dictionary of Military and Associated Terms. As of January 2021, available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (August 18, 2021).

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, available at: http://data.europa.eu/eli/dir/2016/1148/oj (August 18, 2021).

Eling, M. & Schnell, W. (2016) Ten Key Questions on Cyber Risk and Cyber Risk Insurance, In: Sommerrock, F. (ed.) *Ten Key Questions on Cyber Risk and Cyber Risk Insurance* (The Geneva Association – International Association for the Study of Insurance Economics' Zurich), pp. 8-37, available at: https://www.genevaassociation.org (August 18, 2021).

Fadia, A., Nayfeh, M. & Noble, J., (2020) *Public and Social Sector Practice, Follow the leaders: How governments can combat intensifying cybersecurity risks, It is undoubtedly challenging to craft and execute a national cybersecurity strategy. Our research reveals common elements of successful strategies* (McKinsey & Company), p. 5, available at: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks (August 18, 2021).

Ferens, A. (2021) Cybersecurity and cyber risk in integrated and management reports of key service operators, *Theoretical Journal of Accounting*, 45(2), https://doi.org/10.5604/01.3001.0014.9558.

Gassmann, O. (2006) Opening up the innovation process: towards an agenda, *R &D Management*, 36(3), pp. 223-228.

Global Cybersecurity Index 2020 (2021) *Measuring commitment to cybersecurity* (Geneva: International Telecommunication Union), available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (August 18, 2021).

Helbing, D. (2013) Globally networked risks and how to respond, *Nature*, 497, pp. 51-59, available at: http://www.marsh-stresstest.eu (August 18, 2021).

Sun, J., Lei, K., Cao, L., Zhong, B., Wei, Y., Li, J. & Yang, Z. (2020) Text visualization for construction document information management, *Automation in Construction*, 111, https://doi.org/10.1016/j.autcon.2019.103048.

Jarvempaa, S.L & Tanriverdi, H. (2003) Leading virtual Knowledge Networks, *Organizational Dynamics*, 31, pp. 403-412, http://dx.doi.org/10.1016/S0090-2616(02)00127-4.

Kavanagh, K., Bussa, T. & Collins, J. (2021) *Magic Quadrant for Security Information and Event Management*, (Gartner Technical Report), available at: https://www.gartner.com/doc/reprints?id=1-26OLSQ2N&ct=210630&st=sb (August 18, 2021).

Kindervag, J. (2010) *Build Security Into Your Network's DNA: The Zero Trust Network Architecture* (John Kindervag for Security & Risk Professionals), pp. 1-25, available at: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (August 18, 2021).

Le-Nguyen, K., Dyerson, R. & Harindranath, G. (2018) Exploring knowledge management software implementation from a knowing-in-practice perspective, *Inf Syst Front*, 20, pp. 1117-1133, https://doi.org/10.1007/s10796-016-9713-3.

Marsh, S., Atele-Williams, T., Basu A., Dwyer, N., Lewis, P.R., Miller-Bakewell, H. & Pitt, J. (2020) Thinking about Trust: People, Process, and Place, *Patterns*, https://doi.org/10.1016/j.patter.2020.100039.

Naseer, H., Maynard, S.B. & Desouza, K.C. (2021) Demystifying analytical information processing capability: The case of cybersecurity incident response, *Decision Support Systems*, 143, https://doi.org/10.1016/j.dss.2020.113476.

NIST (2020) Security and Privacy Controls for Information Systems and Organizations, *NIST Special Publication 800-53*, Revision 5, (National Institute of Standards and Technology), https://doi.org/10.6028/NIST.SP.800-53r5.

Orenga-Roglá, S. & Chalmeta, R. (2019) Methodology for the Implementation of Knowledge Management Systems 2.0, *Bus Inf Syst Eng*, 61, pp. 195-213, https://doi.org/10.1007/s12599-017-0513-1.

Ostrom, E. (2013) *Dysponowanie wspólnymi zasobami* (Warszawa: Wolters Kluwer).

Chamoso, P., Rodriguez, S., de la Prieta, F. & Bajo, J. (2018) Classification of retinal vessels using a collaborative agent-based architecture, *AI Communications*, 31, pp. 427-444.

Pizło W. & Parzonko A. (2022) Virtual organization and trust, In: Paliszkiewicz, J. & Chen (eds.) *Trust, Organization and Digital Economy* (London: Taylor and Francis), pp. 61-79.

Rashid, Z., Noor, U. & Altmann, J. (2021) Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem, *Future Generation Computer Systems*, 124, pp. 436-466.

Refsdal, A., Solhaug, B. & Stølen, K. (2015) *Cyber-Risk Management* (Cham: Springer International Publishing).

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020) Zero Trust Architecture, *NIST Special Publication 800-207* (National Institute of Standards and Technology), https://doi.org/10.6028/NIST.SP.800-207, available at: https://www.nist.gov (August 19, 2021).

Schmidt, S. & von der Oelsnitz, D. (2020) Innovative business development: identifying and supporting future radical innovators, *Leadersh Educ Personal Interdiscip*, 2, pp. 9-21, https://doi.org/10.1365/s42681-020-00008-z.

Smith, V.L. (2013) *Racjonalność w ekonomii* (Warszawa: Wolters Kluwer).

Snellman, L. C. (2014) Virtual teams: Opportunities and challenges for e-leaders, *Procedia – Social and Behavioral Sciences*, 110, pp. 1251-1261.

The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2., available at: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf (August 19, 2021).

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B. & van Ruijven, T. (2021) Understanding incentives for cybersecurity investments: Development and application of a typology, *Digital Business*, 1(2), pp. 1-7, https://doi.org/10.1016/j.digbus.2021.100014.

Yang, L., Lau, L. & Gan H. (2020) Investors' perceptions of the cybersecurity risk management reporting framework, *International Journal of Accounting & Information Management*, 28(1), pp. 167-183.

Cybersecurity and School-age Young People – Challenges and Threats

ANDRZEJ PIECZYWOK

Abstract Cybersecurity is currently a major priority for states. The Internet is providing growing opportunities for development, but it can also lead to risky situations. As the Web continues to expand, people are more likely to be exposed to threats due to inadequate security or the inappropriate use of resources online. State-of-the-art digital media and interactive information and communications technology – all of which constitute cyberspace and the virtual world – pose many threats for school-age young people. They are dynamic and widespread, and have a global dimension. It is common practice for both teachers and students to use the rich educational resources available online. Against this backdrop, it is important to investigate what causes online threats to emerge and what consequences they have, as well as to develop popular awareness towards a safe use of cyberspace.

Keywords: • cyberspace • cybersecurity • school-age young people • challenges • threats • cybereducation

CORRESPONDENCE ADDRESS: Andrzej Pieczywok, Ph.D., Dr. Habil., University Professor, Kazimierz Wielki University, Faculty of Political Sciences and Administration, Department of Security Policy, ks. J. Poniatowskiego (Street) 12, 85-671 Bydgoszcz, Poland, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

https://doi.org/10.4335/2022.1.14 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

The bulk of human activity nowadays – whether educational, social, professional or leisure – takes place in cyberspace. Professional and school lives, and most social contacts, have largely gone online. On the one hand, this creates enormous opportunities, but on the other, we need to realise that many threats are also involved. In recent years, the information-related dimension of threats has become particularly significant. The Internet, networks, information, data and cyberspace have all become critical for citizen and organisational security and knowledge, and even for the authority of states. Virtual space is very often more attractive than other environments. It allows people to meet many of their needs. Interpersonal attractiveness can grow substantially online (financial and social benefits, improved self-esteem, developing a certain identity, etc.). What counts online is closeness, the law of attraction, humour, civility and mutual sympathy. Indeed, virtual communication clearly has many advantages: anonymity, wide reach, imagination, etc. School-age young people are fairly active on social media. It is worth noting that the main idea behind these sites is to allow users to stay in contact with their friends and relatives, or to make new acquaintances, as well as to share certain information with large groups of people. Sometimes it is difficult to maintain privacy. Social media sites are a real world for many young people. Moreover, they are an ever-changing space in which young people can express their identity and establish relations with others, often from different countries (Kowalczuk, 2009: 25). Social media foster their need for being part of a group, for belonging, being active, establishing their presence and promoting themselves. Young people, in particular, adolescents, tend to have a strong desire to express their views. Through social media sites, they can engage in dialogue and share interesting information – i.e. communication that satisfies their sense of agency and fosters their creative achievements and cause-and-effect thinking.

It is worth noting that cybersecurity means the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. The use of social media sites involves many emerging threats associated with, among others, providing sensitive information to other users (burglars, paedophiles), phishing (access to passwords and logins), identity theft, cyberstalking, talking to strangers, etc. Information technology carries with it many threats whose consequences are hidden and distant in time. It is important to be aware of the threats and to have the knowledge and skills to navigate cyberspace. School-age young people tend to believe that they know more about the Internet than adults, overestimating their online skills and ability to protect against these threats.

Cyberspace addiction is a common problem nowadays. Some compare it to alcoholism and drug addiction. Many young people struggle with computer, TV or mobile phone addictions. They lie to themselves, which makes them oblivious that they have a problem. School-age young people do not realise the underlying threats. The uncontrolled use of media often causes changes in how their body and personality function.

The Internet is the main channel for communication and source of knowledge for young people. Hence, it is critically important for them to develop critical thinking and source verification skills. With the spread of fake news and unverified information, these skills are instrumental in protecting young people against being misled or even manipulated. Knowledge acquired online is currently replacing academic knowledge gained by reading books, encyclopaedia and scientific journals. Whereas these traditional sources are highly reliable and can be trusted, the Internet is a mosaic of information, the control over and verification of which is limited. Therefore, it is critically important for them to develop critical thinking and source verification skills.

2 Main threats associated with the inappropriate use of cyberspace

Cyberspace not only opens up qualitatively new opportunities that can make life easier for people, but also involves a range of qualitatively new threats in the personal, national and even international dimensions. It can be a source of addictions, a vehicle for socially unacceptable behaviours and values, a tool of qualitatively new forms of crime, a space for terrorist activities, and an arena for cyberwarfare if seen through the lens of military threats (Pieczywok, 2017: 113).

Threats associated with the broadly defined human contact with the world of technology, and, in particular, cyberspace, have been engendered by the euphoria surrounding the new opportunities afforded by the world of media. This euphoria has caused people to become less cautious, to underappreciate, and even to consciously ignore threats. As shown by the history of human civilisation, threats are an inseparable part of the encounter with new techniques and technologies. This creates – in quantitative and qualitative terms – new needs, or generates them artificially, indirectly making survival dependent on adaptation – in terms of both broadly defined technology and at the psychological level. These technologically forced shifts may lead to outcomes that are difficult to predict – both globally and individually. As rightly noted by S. Bębas, "technological advancements have changed not only human habits, but also the way in which pathologies can manifest" (Bębas, 2013: 22).

According to M. Szydłowska, information threats are "all destructive (intentional and unintentional) acts in the form of the undesirable disclosure, distortion, modification, damage, destruction, or the disabling of the processing of, information produced, processed, stored, and sent in a specific information flow system, potentially causing a loss (Szydłowska, 2019: 22).

P. Bączek claims that, when analysing information security, the following threats should be addressed: 1) random (natural disasters, catastrophes, accidents, fires, floodings); 2) conventional (espionage, subversion, sabotage, disinformation); 3) technological (cybercrime, cyberterrorism, information warfare); 4) civil rights-related (unauthorised disclosure, information selling, breach of privacy, unlawful interference by special forces,

thwarting public transparency); 5) organisational and structural shortcomings (mishandled operations, mismanagement and poor decision-making, poor information flow, corruption) (Bączek, 2005: 71-73).

Adverse phenomena associated with the development of information technology and, by extension, cyberspace, include: 1) the decline of humanistic values – technocratic outlook on the world; 2) opportunities to manipulate people freely – to steer their consciousness; 3) difficulties adapting to an information society and addiction to technology; and 4) the spread of pathological processes associated with the use of technology, such as violence, aggression, erotica and pornography, piracy and hacking, computer addiction (Siemieniecki, 2001: 31).

Cyberspace threats are multidimensional. These do not just pertain to access to inappropriate content, but also to the risk of eye and musculoskeletal diseases, and mental diseases. Of particular concern are addictions and, increasingly, specific behaviours associated with different types of violence and aggression (in both the virtual and real world), social changes and ethical threats, as well as the decline of independent thinking and deep reflection.

Threats may come from unverified software downloaded by students and teachers, fake websites, links to malicious codes and malicious codes contained in attachments to emails offering discounts for teachers, or fake emails from IT departments. Sensitive information about students, teachers and graduates are of great value to hackers – they can demand money to decipher such information or sell it on a black market. The research results and intellectual property of educational institutions are targeted as well.

As far as education is concerned, particular dangers relate to the cognitive and intellectual sphere involving cognition and school learning, which include: cognitive threats (uniformity and/or reduction of experience), limited perception of issues, the primacy of visual over verbal, inundation with ready-to-use hypermedia information, preventing their creative shaping and use, and the inability to take rational decisions and actions (Pieczywok, 2017: 114).

Generally, cyberspace threats to school-aged young people can be divided into a number of primary areas. These include: 1) cyberspace threats: a) mental and physical health threats: eye ailments, hearing disorders, musculoskeletal ailments, wrist ailments, thumb ailments (texting), diseases of other body organs, self-destruction, self-harm, cyberspace suicide; b) moral threats: cyberpornography, online prostitution; cyberpaedophilia, cybersex, sexting, human trafficking, including for organ trade; c) socio-educational threats: cyberbullying, online violence and aggression, gambling, second life, cybersectarianism, human trafficking, including for organ trade, impaired interpersonal relationships, human functioning in the world of humanoid robots; d) chemical hazards: bigorexia, drugs online, energy drinks, new psychoactive substances; and e) infoholism and computer-game threats; as well as 2) crime and ICT security threats: a) ICT crime in

the EU; b) ICT security policy, including: - violating the integrity and confidentiality of, and disabling access to, data and computer systems; - computer crime; - crime specific to the nature of targeted information; - intellectual property crime; c) ICT crime in Poland, including: - crime against information protection, - computer hacking, - electronic eavesdropping; - unlawful destruction of information; - computer sabotage; - copyright violation, - crimes against the credibility of documents; and d) virtual financial crime. Among school-age young people, these threats can take the form of an addiction, necessitating measures to prevent, diagnose and treat threats and pathologies.

3 The cybereducational dimension of shaping attitudes in school-age young people

It can be assumed that education is a unique socio-cultural process through which humans gradually develop, mature and shape their personality. The educational system allows young people to establish social relationships and gain socio-cultural experience (Tkacz, 2008: 315).

For a long time, the aim of education was to facilitate the acquisition of certain information, skills and attitudes. Nowadays, however, its main priority is not to pass encyclopaedic information, but to shape attitudes. Accordingly, the qualities that are now fostered by education include being active, having imagination, being intellectually autonomous, and engaging in continuous education.

It is clear, then, that school education related to identifying and counteracting cyberthreats improves the effectiveness of help and support to school-age young people experiencing virtual-world problems. Thorough knowledge about the psychological mechanisms underlying addiction and co-addiction, and the ability to apply it in everyday work with students, are very important.

As human civilisation continues to develop, the educational system has no choice but to follow. Digitisation, digital teaching, mixed learning styles, cyberspace learning and mobility have all become a part of the educational routine. Nevertheless, there exist some deeply ingrained and persisting habits causing teachers to be viewed through the lens of the system as compliant cogs, deprived of any tools – a part of a mindless testing machine. Embracing these new developments while overcoming the deep-seated mindset is a challenge for teachers. Usually, however, change is not entirely possible even if there is willingness to make it.

The constantly evolving digital technology and very easy access to diverse information engender the misconception that, for instance, the Internet and e-learning are fully sufficient to teach more in less time. There is no denying, however, that the ongoing ICT revolution will force profound changes across formal and informal education, mainly in the choice of educational contents, the teaching-learning methodology, and in evaluating school performance. Media pedagogy is facing the serious challenge of actively shaping

indispensable human skills. This mainly involves improving the ability to actively and creatively participate in developing the culture of network society. School and broadly defined education will certainly come under criticism. There is no doubt, however, that teachers will manage to mould information acquired by young people from a wide range of sources into the sound knowledge they will especially need in the future (Pieczywok, 2017: 120).

Today's schools provide students with inadequate – or, to be more exact, very little – preparation to handle the emerging challenges associated with ICT threats, addiction to new technology, and cyberspace pathologies. It should be kept in mind, however, that nobody prepared teachers (educators) and parents for these new tasks. Schools lack experts and teachers capable of diagnosing issues among students exposed to cyberspace threats. For these reasons, online security and safety in the context of the threats and social pathologies is emerging as the latest and highly important educational problem and challenge for teachers. Hence, as rightly noted by J. Kopański – "preparation for the teacher profession and the continuing professional development among teachers must change to take account of the ongoing evolution in the use of media" (Kopański, 2010: 83).

It is not common for teachers and students to have adequate knowledge about the functioning of social media sites, about using the potential of the Internet, and about online safety. As online crime, addiction to the Internet, and the adverse impacts of the Internet on behaviour become a growing phenomenon, the role of media education at school is coming to the fore (Goban-Klas, 1999: 49).

Hence, providing the general public with media education is now an important challenge. Contemporary school is being profoundly influenced by the Internet, perhaps to the point of being under its dictatorship. What is interesting is that not only pupils and students but also teachers succumb to this dictatorship. For many years now – in fact, from the dawn of computers and later the Internet – education has been constantly adapting to the world of technology.

In the face of the technological advancements and increasing digitisation, there is an ever-growing need for raising awareness about cyberthreats and for education in this area among young people.

In the context of these threats, it is particularly important to provide cybereducation understood as the diagnosis, prevention, and therapy at institutions dealing with the education and socialising of school-age young people, including family, schools, media, counselling centres, foundations, organisations, etc.

It is important that school curricula incorporate instruction on cybersecurity, which is becoming one of the primary challenges of the 21st century. Cybereducation should become a permanent part of the school landscape, especially in the form of practical

classes to teach young people how to use the Internet safely. While the user is usually the weakest link in each system, cybereducation among students and teachers is still lacking. Therefore, it is important to show teachers and students what to pay attention to, what information and applications should raise suspicions, and to whom to report incidents. It is not enough to give a 15-minute talk at the beginning of the school year. What is needed is ensuring continuous cyberhygiene care.

The aim of cybereducation is to make sure young people know how to use online resources safely, where to look for help when they fall victim to cybercrime, and how to critically approach information found on the Internet.

The basic skill that young people should learn is to remain aware of how the information they share online, almost on a daily basis, can be used. For instance, pictures of them walking their dog, photos of expensive gadgets, and logging in at specific locations can help criminals determine, for one, their daily routine. Another fundamental task is to teach school-age young people to identity attempts to illegally obtain information.

Education will certainly face the challenge of adapting instruction plans to the dynamically changing landscape of threats and methods used by criminals. Caution should be at the core of students' activities online. Being careful, however, is not enough. It is fundamentally important to instil in them scepticism about sharing their sensitive data online. Everyone should also form the habit of protecting their information, and learn how to create strong passwords. While this might seem obvious, it is still common for students to use weak combinations and log in at various locations using the same identification data.

A growing number of teachers and experts are realising that the issue of cybersecurity is underestimated at schools. Cybersecurity instruction could take place during weekly class meetings, computer science classes, or as part of a dedicated subject. It should be borne in mind that lectures and routine school talks are not enough. One way to mobilise young people to explore the subject deeper would be to organise contests and practical classes for them. In fact, there are a myriad of possibilities to tackle this challenge.

Cybersecurity education should be provided as soon as children and young people gain access to digital services, preferably before they even enter the digital world, i.e. at preschool. There is a need for a wide social campaign on cybereducation and cyberhygiene. To make this happen, a multi-pronged approach should be taken by incorporating cybersecurity into the core curriculum and securing adequate funds to improve teacher competencies, among others. This would involve developing and implementing a continuous teacher development programme on using new technology, and supporting them in meeting core-curriculum requirements related to the safe use of new technology.

The combination of the teacher's professional knowledge and deep experience allied with the digital skills of students and opportunities afforded by digital devices creates a true synergy in shaping modern education and educating a generation that will change the world more consciously and responsibly. Jan Wróbel is right to claim that "in the school of the future, it is the teacher that is, or at least should be, of prime interest" (Wróbel, 2010: 67).

Routine tasks performed by teachers should be increasingly replaced with attractive computer programs, especially given the now fairly common availability of virtual lectures, modern e-learning courses, instructional games, electronic tests, educational portals, as well as digital school registers and systems designed to monitor the learning process. Indeed, for many students, a multimedia lecture is much more interesting than a regular class. Teachers are not, therefore, needed to pass knowledge, test and evaluate. Their new role involves acting as advisers, coaches, counsellors and learning experts, supporting students in difficult moments, guiding and motivating them when in doubt, and teaching them how to learn.

As new information and communication technologies and cyberspace continue to evolve, the role of teachers is changing. As well as being able to use cyberspace tools, teachers should know the threats posed by cyberspace to respond appropriately when seeing adverse cyberspace-related effects in their students. Also, in addition to passing on the latest knowledge, their role is to protect children against negative phenomena in cyberspace. In order to provide such protection, however, they need to become familiar with the origin, scale, causes and effects of these phenomena.

When providing education with the use of latest information technologies, to shape desirable attitudes in school-age young people, teachers should not only provide them with the right conditions to acquire knowledge and the practical skills to apply it, but also shape their moral qualities, such as honesty, reliability, responsibility, etc.

It is worth stressing that digital space, the virtual world and the Internet are changing the lifestyles and culture of learning of both teachers and students, as well as the way they communicate. Hence, the following should be at the core of educating the young generation as a conscious information society: 1) promoting critical attitudes towards content found in cyberspace and the ability to cull through the content; 2) forming an active attitude to cyberspace resources to make it a tool for actively influencing audiences; 3) stimulating and strengthening sensitivity to providing objective information and promoting attitudes against its distortion; and 4) passing on knowledge of cyberspace specifications and its underlying mechanisms (Trzcińska, 2006: 269).

4 Conclusion

The potential of technology and online resources, teenager habits shaped by their contact with technology and the power of teachers' expert knowledge should create a new space for learning and a new model of working. Parents and teachers will, thus, together face the challenge of implementing innovative project methods and preparing students for work.

In addition to a range of advantages, the use of cyberspace by students has a fair share of negative aspects. The threats that await us online, including, in particular, that faced by children and young people, are increasingly serious, and it is impossible to protect young users against them only by using software to block undesirable websites.

Today, the key factor in school-age young people's development is having the ability to use, analyse, creatively process and appraise information. Media digitisation has made it possible to create virtual reality, leading to a life in the so-called "simulacrum culture". This is why reflective thinking, nurturing imagination, and developing the ability to distinguish facts from fiction are important.

References:

Bączek, P. (2005) *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego* (Toruń: Wydawnictwo Adam Marszałek).

Bębas, S. (2013) *Patologie społeczne w sieci* (Toruń: Wydawnictwo Edukacyjne „AKAPIT").

Goban-Klas, T. (1999) *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania* (Warszawa: Wydawnictwo Fundacji Postępu Telekomunikacji).

Kopański, J. (2010) Kompetencje nauczyciela a cyberbezpieczeństwo ucznia, *Meritum*, 4, pp. 82-87.

Kowalczuk, P. (2009) Posługuje się myszą i klawiaturą, *Wychowawca*, 9, pp. 25-26.

Pieczywok, A. (2017) Edukacyjne wyzwania w kształtowaniu pozytywnych postaw młodzieży w cyberprzestrzeni, In: Trubalska, J. & Wojciechowski, Ł. (eds.) *Bezpieczeństwo osób w cyberprzestrzeni* (Lublin: Wydawnictwo Wyższej Szkoły Innowacji i Ekonomii), pp. 107-126.

Siemieniecki, B. (2001) *Technologia informacyjna w polskiej szkole. Stan i zadania* (Toruń: Wydawnictwo Adam Marszałek).

Szyłkowska, M. (2019) *Bezpieczeństwo informacyjne państwa. Wybrane problemy* (Toruń: \Wydawnictwo Adam Marszałek).

Tkacz, T. (2008) Formalne i prywatne funkcje przestrzeni edukacyjnej, *Nierówności Społeczne a Wzrost Gospodarczy. Uwarunkowania Instytucjonalne*, 12, pp. 315-320.

Trzcińska, M. (2006) W stronę pedagogiki mass mediów, In: Muchacka, B. (ed.) *Szkoła w nauce i praktyce edukacyjnej* (Kraków: Oficyna Wydawnicza „Impuls"), pp. 265-273.

Wróbel, J. (2010) *Nauczyciele, supermani i poczciwe niezguły* (Gdańsk: Wydawnictwo Aeropag).

Institute for Local Self-Government Maribor

www.lex-localis.press
info@lex-localis.press