LEX LOCALIS

Cybersecurity in the Visegrad Group Countries

Authors:
András Bencsik
Mirosław Karpiuk
Miroslav Kelemen
Ewa Włodyka


§
LEX
LOCALIS

Title: Cybersecurity in the Visegrad Group Countries

Authors: assoc. prof. András Bencsik, Ph.D., Dr. Habil. (Eötvös Lóránd University, Faculty of Law, Hungary), prof. Mirosław Karpiuk, Ph.D., Dr. Habil. (University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Poland), prof. Miroslav Kelemen, Ph.D., Dr. Habil. (Technical University of Košice, Faculty of Aeronautics, Slovak Republic), Ewa Włodyka, Ph.D. (Koszalin University of Technology, Faculty of Humanities, Poland)

Reviewers: prof. Dr. Habil., István Hoffman (Eötvös Loránd University (Budapest), Faculty of Law, Hungary), assoc. prof. Dr. Habil., Jarosław Kostrubiec, Ph.D. (Maria Curie-Skłodowska University (Lublin), Faculty of Law and Administration, Poland)

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani

COBISS.SI-ID 160812035
ISBN 978-961-7124-17-0 (PDF)

First Published in 2023 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 "Cybersecurity in the Visegrad Group countries" supported by the Institute for Local Self-Government Maribor, Slovenia.

https://doi.org/10.4335/2023.6 ISBN 978-961-7124-17-0 (PDF)

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

Cybersecurity in the Visegrad Group Countries

Authors:
András Bencsik
Mirosław Karpiuk
Miroslav Kelemen
Ewa Włodyka

Maribor 2023

LEX LOCALIS

Cybersecurity in the Visegrad Group Countries

ANDRÁS BENCSIK, MIROSŁAW KARPIUK, MIROSLAV KELEMEN & EWA WŁODYKA

Abstract To ensure a high level of cybersecurity, the legislator, both at the level of the European Union and within individual states of the Visegrad Group, has introduced certain solutions to adequately protect information systems, imposing an obligation to take measures to secure these systems against unauthorised interference. Incidents can significantly reduce the performance of information systems due to their vulnerabilities. Therefore, any duties connected with countering incidents which may compromise cybersecurity must be adequate to the importance of tasks performed using these systems.

Ensuring and maintaining a high level of security in cyberspace requires individual countries to set fundamental objectives in this field. These objectives are outlined in national cybersecurity strategies. The EU legislator makes it clear that these strategies should not only address the priorities for cybersecurity activities or identify risk management issues and actors, along with their competencies in the domain of cybersecurity, but also define response and recovery measures, the scope of cooperation between public and private sectors, as well as the guidelines for information, training and educational programmes, or recommendations for scientific research projects.

Keywords: • Visegrad Group countries • cybersecurity • cyberspace

CORRESPONDENCE ADDRESS: András Bencsik, Ph.D., Dr. Habil., Associate Professor, Eötvös Lóránd University, Faculty of Law, Department of Administrative Law, Egyetem tér 1., H-1053 Budapest, Hungary, e-mail: bencsik.andras@ajk.elte.hu, ORCID: 0000-0001-5772-9968. Mirosław Karpiuk, Ph.D., 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. Miroslav Kelemen, Ph.D., Prof. Ing. DrSc., Full Professor, Technical University of Košice, Faculty of Aeronautics, Rampová 7, 041 21 Košice, Slovak Republic, e-mail: miroslav.kelemen@tuke.sk, ORCID: 0000-0001-7459-927X. Ewa Włodyka, Ph.D., Koszalin University of Technology, Faculty of Humanities, Department of Political Science, ul. Kwiatkowskiego 6e, 75-343 Koszalin, Poland, e-mail: ewa.wlodyka@tu.koszalin.pl, ORCID: 0000-0002-8229-342X.

https://doi.org/10.4335/2023.6 ISBN 978-961-7124-17-0 (PDF)

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

Table of Contents

Introduction

Due to ongoing technological changes and the widespread digitisation of public and private life, all countries must protect their citizens and institutions from cyber threats which can have far-reaching consequences, including those related to the destabilisation of the economy or the functioning of public power. This digitisation is made possible thanks to the widespread use of ICT systems, not only for fast and remote communication but also as part of conducting business activities and implementing public tasks. As these systems are sensitive to disruptions, both the state itself and private entities (especially those providing essential services) must use their best endeavours to minimise these disruptions which, in some cases, can significantly limit the ability to perform tasks (including those that are critical to the proper functioning of the state and to address the needs of society) or to provide services (including those related to business activity), as well as the ability to communicate.

By recognising the advantages of an information society, individual states should be engaged in its development. The measures taken and the means used to this end highlight the important role that is nowadays played by cyberspace, which mainly stems from the expansion of global ICT networks connecting millions of users and enabling communication between them. This development is directly connected with the technological transformations that have taken place in the field of electronic communication and, in particular, information and communication technologies (Chałubinska-Jentkiewicz, Brzostek, 2021: 5).

The dynamic development of ICTs has contributed to the emergence of a new field of activity, namely cyberspace, as being one of the underlying changes in the security environment entailing completely new threats (Pieczywok, Kościelny, Wasilewski, 2021: 70). Cyberspace is the domain where activities are carried out in the public, private, social and economic spheres. It is used to provide various types of services and communication. Its importance for the state and society is very high, which is why public and private institutions (including operators of essential services or digital service providers) have to protect it. Security against cyber threats must be one of the priorities of state policies, as well as the duty of those responsible for ensuring the security of information systems (Karpiuk, Kelemen, 2022: 71). Cyberspace is a global network consisting of interconnected ICT networks made up of devices that enable the creation, processing and exchange of information automatically between devices, or knowingly and intentionally between their users. Defined in this way and constituting the domain of everyday activities of both states and their citizens, in which vital interests are pursued, cyberspace is under constant threat posed by the illegal activities

of individuals and groups, as well as system errors or failures (Milik, 2021: 12). In connection with globalisation and the widespread use of ICT systems, the protection of cyberspace has become one of the state's primary security tasks.

The information revolution, the creation of the Internet, the development of an information society, the globalisation of virtually all spheres of human activity, and the accompanying rapid technological progress are undoubtedly among the main trends shaping the contemporary information environment. This has resulted in the emergence of cyberspace – a global space that is not limited by time or borders, or by geographical or political factors (Chałubińska-Jentkiewicz, Karpiuk, Kostrubiec, 2021: 29). The advantage of cyberspace, which allows it to be used to pursue a type of warfare, is a lack of spatial limitations, i.e., the lack of a specific territory. Importantly, there is a large amount of information that can be eliminated or acquired from cyberspace by maintaining anonymity and concealing the methods and tools used, which limits the prospects of real-time response (Stolarz, 2021: 13). At this point, it is important to note the specific nature of cyber threats which tend to have cross-border character and, therefore, are not limited to individual jurisdictions. This leads to the internationalisation of both the attacks themselves and the response to them, along with their impact on the operations conducted by individual states (Pelc, 2022: 60).

The development of new technologies necessitates the search for new solutions to ensure the security of activities undertaken in cyberspace (Hoffman, Karpiuk, 2022b: 173). The dynamics with which the solutions offering protection against cyber threats are applied must be adequate to, or even ahead of, the dynamics of the cyber threats themselves. The tools that are used should offer protection against threats, rather than merely enabling their identification, elimination or prosecution of perpetrators. And this requires adequate financial investments in the purchase of modern cyber solutions and qualified staff as well.

Professional staff who carry out tasks in the field of cybersecurity and, at the same time, have the adequate knowledge and skills, or the adequate competencies, guarantee the suitable quality of the measures taken to secure cyberspace against attacks, thus contributing to the optimisation of its functioning which, in turn, enables cutting the disruptions occurring in that domain to the minimum (Bencsik, Karpiuk, 2023: 83).

The challenges emerging in the new digital age have resulted in the transformation of the functioning of public institutions, including administration authorities (Hoffman, 2021: 157). Digital transformation has also covered society whose needs are being increasingly addressed by public administration using cyberspace. The administration must, therefore, satisfy the requirements set by the information society, thus meeting the needs of that society.

Chapter I

Cybersecurity in Hungary

1 Introductory thoughts

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

For the sake of completeness, however, the author of this work cannot fail to highlight the undisputed virtues of optimal digitisation of public administration, which are also relevant to our publication. The leading foreign literature is unanimous in the view that the use of proven digital tools can have a pull effect, which can legitimise the use of new technological tools in new sectors not previously affected by digitisation. This effect is reinforced by the fact that standardised platforms and other digital solutions from the competitive sector can be easily transferred to public administrations, within certain scope and under certain conditions. It is in fact the case that this intermediary, interactive online value creation activity is a phenomenon also known in the „traditional" offline economy, which as a rule operates on the technology and infrastructure of a business (Firniksz, 2021: 171-173).

On the other hand, it should also be stressed that technological tools, especially in the field of public administration and the organisation of public services, can be increasingly used to achieve and strengthen the objectives declared as goals to be achieved by national and EU public administration policies (e.g. customer orientation, efficiency, subsidiarity, etc.). In this context, we would refer to the indicators of the Digital Economy and Society Index (DESI), which ranks the countries of the Central and Eastern European Union in the bottom third of the scale, particularly in terms of the efficiency of public services. According to the index, Hungary ranks 23rd, Slovakia 24th, Poland 25th and the Czech Republic 18th, with slightly better indicators.

It should also be pointed out, however, that digitisation is not just a matter of the functioning of the State and the development of public services: in addition to civil administration, the use of new technologies is also becoming increasingly important in

defence administration (including defence and the conduct of military operations). There are legal, IT and military aspects to this, which are worth examining and which could also be used to fine-tune the regulatory environment. It should be noted that the issue of new technologies and, more specifically, cybersecurity, is linked to the world of criminal sciences in a number of ways which, for reasons of space and looser links (Szathmáry, 2021: 642-650), are not the subject of this paper (Mezei, 2019: 305-314).

It is also worth pointing out that, however inevitable the emergence of the digital explosion in the public sector may be, experience to date - especially in the CEE region - does not necessarily suggest that it is a complete success story. The reasons for this include the difficulty of taking organisational and procedural aspects into account at the same time, the slow and costly process of building infrastructure, and the general resistance to change (especially in human resources), which is also a classic barrier to innovation. Unfortunately, the military-defence aspect, which is the subject of this chapter, has, however, extensive experience and international reactions, which show that cyberspace is (has been) more receptive to the application of the technologies indicated than civil administration. Another unfortunate development in Hungary is that several articles have recently been published which - in addition to presenting the results achieved – emphasise why there is no need or opportunity for further digitisation in public administration.

2 On military cyber defence

The military aspects of cyber defence have become an inescapable priority in the framework of NATO (and Hungary as part of it) defence management. Behind this trend is the realisation that, following the end of the Cold War, cybersecurity activities pose the greatest risk, with cyber warfare emerging as a new phenomenon, with operational effects in cyberspace (Tóth T., 2018: 49). The question rightly arises as to what are the specific characteristics of cyber warfare that justify a completely new basis for defining the nature of military operations (and defence). There seems to be a consensus in the authoritative literature that the defining characteristics of cyber warfare are: 1) there are no national borders (this is essentially a consequence of the borderless nature of cyberspace and the diversity of attacks); 2) the warring parties include not only military but also civilian actors (espionage, disruptive or destructive goals are often achieved by involving hacker groups); 3) participants and destinations include international companies, domestic and international service providers and global services.

Hungary has been a member of the North Atlantic Treaty Organisation (NATO) since 1999, and therefore Hungary could not have been unaffected by the trends and reactions that have emerged in recent years in relation to cyber warfare within NATO. NATO was confronted with cyber warfare for the first time this year, following the bombing of Kosovo, and the cyber attacks detected were carried out initially by the Serbian hacker group Black Hand, and then by Chinese and Russian hackers following the bombing of

the Chinese Embassy. The story had both indirect and direct international consequences. The following developments are worth highlighting: 1) following the 2002 NATO summit in Prague, the development of a NATO cyber defence policy came to the fore (Tóth, 2016: 214); 2) at the 2014 Wales Summit, NATO's cyber defence policy guidelines were adopted and cyber defence was included in the collective defence tasks; 3) in 2016, in the final document of the Warsaw Summit, the Allies extended the scope of operational warfare to cyberspace and declared that a cyber-attack against a NATO member state could be considered an attack against the Alliance as a whole and could be subject to collective response if necessary; 4) at the 2018 Brussels Summit, it was declared that, while NATO is focused on developing collective defence cyber capabilities, member states are building a full range of capabilities for deterrence and effective action.

To conclude this reflection, it is also worth pointing out that, in addition to cyber warfare, cyber diplomacy (Nyáry, 2020: 332) is increasingly emerging as an instrument of state foreign policy, which can be defined as the use of diplomatic resources and procedures to promote national interests in cyberspace (Kerekes, 2021: 36-38).

3 Cyber defence and information security in Hungary

In terms of risks to national security, there are a number of factors that require a cybersecurity toolkit and approach to address, and the domestic legislator needs to be constantly prepared and responsive. In this context, the European Union dimension is of crucial importance, forcing Member States, including Hungary, to constantly re-think. In this context, it is worth mentioning the launch of the Critical Infrastructure Regulation, which was "launched" by the Justice and Home Affairs Council in December 2005, which invited the Commission to present a proposal for an EU programme for the protection of critical infrastructure. In this context, two comments should be made: firstly, the European Programme for Critical Infrastructure Protection (EPCIP) is based on a comprehensive threat approach and, secondly, it is the framework for the pioneering Directive 2008/114/EC, which for the first time mentions the European Critical Infrastructure (ECI) category (Tóth A., 2017: 21). Among the most important EU cyber defence nodes, the following are worth highlighting: 1) tightening cybersecurity rules to address the threat of cyber-attacks and harness the opportunities of the digital age; 2) the establishment of a Cybersecurity Industry, Technology and Research Centre, which is expected to improve the coordination of cybersecurity research and innovation; 3) implementing horizontal measures in the fight against organised crime, among others; 4) the creation of a European Union Cybersecurity Agency to support Member States in dealing with cyber-attacks: as a consequence of the latter development, the National Cyber Defence Institute was created under the auspices of the National Security Service on 1 October 2015 (Csányi, 2021: 476-477).

For reasons of scope, the present work cannot provide an overview of NATO's cyber defence activities, so we will focus on the legislative developments made by the

Hungarian legislator to achieve the Alliance's objectives. Among the Hungarian legislative developments, the present study will focus on a relatively new piece of legislation catalysed by NATO's cyber defence policy, namely Act L of 2013 on the Electronic Information Security of State and Local Government Bodies.

The rationale behind the adoption of the legislation is essentially based on the recognition that Hungary, like many other countries in the world, considers cybersecurity a national security issue of high priority (Krasznay, Muha, 2013). The legislation is both new and old: while it can be noted that information security regulation in Hungary dates back 30 years, the legislative product under consideration can be considered novel in several respects. In this respect, the novae can be identified below: 1) no legislation had previously regulated the IT security of public administrations; 2) since then, there has been a separate regulation on critical infrastructure protection, with which the protection of critical information infrastructure fits in; 3) there have been bodies in the past that have (also) dealt with cyber defence, without a legal basis, in the absence of regulation. Here we mention the National Security Service, of which the National Cyber Defence Institute is now part.

The legislation has been the subject of serious professional-political debates in the literature and (in the legislative debate) among certain opposition parties, even before it was actually applicable. One of the most serious concerns is the scope of the law, since at the time of its adoption there was no inventory of critical information infrastructures, which meant that the legislator was forced to designate these actors, in terms of legal security. This obligation was fulfilled by the legislator with the creation of Government Decree No. 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and installations.

The other key issue of the reservations is the so-called "Big Brother" effect, the real risk of which is not yet supported by a legal context: on the one hand, it should be stressed that the authorities have had legal means to monitor the electronic activities of certain citizens, and on the other hand, according to some representatives of the literature (Krasznay, Muha, 2013), it is precisely a properly functioning information security system that can provide a control that can strengthen the transparency of organisations.

4 New regulatory directions in Hungary

With the rapid digital transformation of society and the ever-intensifying use of new technologies, electronic information systems and digital tools have undeniably become central to everyday life. This development has also led to an increase in the range of digital threats, which can pose risks in several respects: firstly, they can hamper economic activity, secondly, they can cause financial losses and thirdly, they can undermine user confidence, causing significant damage to both economic and social life. Beyond this general observation, cybersecurity is a key factor for many critical infrastructure-based sectors to successfully embrace the digital transformation and fully

reap the economic, social and sustainable benefits of digitalisation. Recognising this, the Hungarian Parliament has set itself the goal of (re)regulating this area and is discussing the draft law T/3314 on cybersecurity certification and cybersecurity supervision as a pending proposal at the time of writing this chapter. In the following, we highlight the main thematically related elements of the draft.

The text of the standard contains extensive definitions to provide a conceptual apparatus for cyber defence regulation. Without describing them, it is possible to indicate that, rather than precise definitions, the terminology used and recorded in sectoral legislation is clarified, which is a step forward in terms of conceptual consistency, but far from clarifying the content.

In the general remarks, it is appropriate to frame the scope of the legislation, according to which the provisions of the General Administrative Procedure Act in the administrative procedures covered by this Act are replaced by the provisions of this Act, the Consumer Protection Act, the Act on the Market Surveillance of Products and the Act on the Authority for the Surveillance of Regulated Activities, as well as the Government Decree on the Rules for the Protection of Civil Aviation and the Regulation on the Powers, Tasks and Functioning of the Aviation Security Committee and the Act on the Authority for the Surveillance of Regulated Activities (hereinafter referred to as the "Act"): shall be applied with the additions contained in the Decree issued by the President of the Air Safety and Civil Aviation Authority. In essence, this can be interpreted as the general procedural code in this sector functioning as a general background norm, but being fleshed out and supplemented by the sectoral procedural rules contained in the said norms.

5 On cybersecurity oversight

As regards the sector under review, it should be noted that the role of the supervisory authority is played by the Authority for the Supervision of Regulated Activities (hereinafter: the "RAO"), as an independent regulatory body, whose chairman has the power to issue regulations (this will be of importance later). The text of the draft standard first discusses the scope of those subject to cybersecurity supervision as follows: the related provisions apply to the electronic information systems of service providers and organisations operating in the high-risk sectors as set out in Annex 1, (examples include: the electricity company, the railway network operator, the pharmaceutical wholesaler, the electronic communications provider and the cloud service provider and to the electronic information systems of service providers and organisations operating in the high-risk sectors as set out in Annex 2 (these include, among others, waste services, chemicals, electrical equipment manufacturing and online marketplace services). However, the draft also emphasises that these rules do not apply to micro and small enterprises within the meaning of the Act on Small and Medium-Sized Enterprises and Support for their Development, unless the organisation concerned: 1) electronic communications service provider; 2) trusted service provider;

3) DNS service provider; 4) top level domain name registrar; 5) domain name registration service provider.

The rules in this Chapter shall not apply to: 1) the electronic information systems and networks of the organisations referred to in paragraph (1) for defence purposes pursuant to the Act on the Electronic Information Security of State and Local Government Bodies; 2) for the protection of programmable systems covered by the Government Decree on physical protection and the related licensing, reporting and control system in the use of nuclear energy, and of system elements designated as European or national critical system elements under the Act on the Identification, Designation and Protection of Critical Systems and Installations, or under the Act on the Identification, Designation and Protection of Critical Systems and Installations.

6 General requirements for those involved in supervision

The organisation concerned shall ensure the security of its electronic information systems and their physical environment in a manner proportionate to the damage caused by cyber threats. This requirement shall include the protection of electronic information systems and their physical environment from any event that could compromise the confidentiality, integrity and availability of data, information stored, transmitted or processed, or services provided by or accessible through electronic information systems. The standard text also makes it clear that the protection indicated must include: 1) the information security management system; 2) identify and manage risks in electronic information systems; 3) the use of administrative, logical and physical measures to mitigate risks, appropriate to the security class to be defined in the organisation's risk analysis for each system; 4) prevent, detect, manage and mitigate the effects of security incidents; 5) ensure business continuity; 6) the acquisition, development and operation of electronic information systems and the software and hardware products they use.

It is of guarantee significance that if the organisation concerned uses a contractor for the establishment, operation, maintenance or repair of the electronic information system, the above requirements must also be met by the contractor. In order to achieve this, the responsibilities and powers of the head of the body concerned are defined, according to which: 1) defines the tasks and responsibilities of the person responsible for the security of electronic information systems; 2) sets out the rules applicable to users of electronic information systems; 3) ensure that the organisation's staff receive regular information security training and keep their knowledge up to date.

Recognising the cross-sectoral nature of cybersecurity, the draft also sets out the principle that the organisation concerned must classify electronic information systems and the data stored, transmitted or processed on them into a security class based on a set of criteria defined in a decree of the Minister responsible for the management of civil national security services (currently the Minister heading the Prime Minister's Office), resulting in a "basic", "significant" or "high" security class based on the risk of

confidentiality, integrity or availability compromise. The specific security measures applicable to each security class are laid down in a decree by the Minister responsible for the management of civil national security services.

The relevant entities identified in the Regulation of the President of the SCCS shall be obliged to use an ICT product, ICT service or ICT process certified under a European or national certification scheme, as identified in the Regulation of the President of the SCCS. Domain names registered under the Top Level Domain shall be kept in a central register by the Top Level Domain Registry, which shall contain: 1) the domain name concerned; 2) the date of registration; 3) the name, contact email address, telephone number of the registrant; 4) the name, email address and telephone number of the person who is the contact point for the domain name, if different from the registrant.

In order to ensure the authenticity and integrity of the data of the central domain name registry, the Top Level Domain Name Registrar shall draw up procedures and publish them in a set of rules and regulations approved in advance by the SCSO. In order to ensure publicity, which is of paramount importance for cyber protection, the text of the Regulation stipulates that the Top Level Domain Registrar shall make the data contained in the central domain name registry publicly available, with the exception of personal data. In addition, it is guaranteed that the Top Level Domain Registry will provide direct access to the data contained in the central domain name register to the public prosecutor's office, national security services, investigative authorities and organisations conducting preparatory proceedings.

7 Cyber security monitoring tools

With regard to the requirements we have mentioned above, the cybersecurity oversight of the relevant entities and their electronic information systems shall be carried out by the SZTFH in accordance with the Decree of the President of the SZTFH. The fulfilment of the obligations of the relevant entity under this Chapter shall be monitored by the SZTFH in accordance with the Decree of the President of the SZTFH.

In the exercise of its cybersecurity oversight powers, the CSA may conduct an official audit of the entity concerned, an extraordinary audit or an extraordinary audit in the event of a significant security incident or suspected non-compliance with security requirements.

The use of the sommat procedure is excluded in the procedure of the SCFH. This essentially means that the procedure cannot be completed within 8 days and is therefore subject to the general time limit. The time limit for the administrative control carried out by the SZTFH is 120 days (this is important because according to the General Tax Code it would be 60 days, but the sectoral procedural rule may differ.

The SZTFH is entitled to request and obtain the information from the organisation concerned, stating the purpose: 1) documents supporting the adequacy of the security classification and security measures; 2) a document on the implementation of the internal IT security audit; 3) any other data, information, documents for the purpose of carrying out the monitoring tasks.

Every two years, the entity concerned shall have a cybersecurity audit carried out by an independent auditor (hereinafter referred to as "the auditor") authorised to carry out the activity to demonstrate compliance with the cybersecurity requirements under this Act. In carrying out the audit, the auditor shall verify the adequacy of the security measures according to the security classification. In order to verify compliance, the auditor shall be authorised to carry out the following tests in a manner that is appropriate for monitoring the activity: 1) internal IT security and remote vulnerability testing, and intrusion testing for "significant" or "high" security class; 2) cryptographic compliance testing; 3) in the case of a "significant" or "high" security class, the security source code review of custom software performing critical security functions.

A cybersecurity audit may be conducted by an auditor who has the expertise and infrastructure necessary to perform the task and is qualified as an entity entitled to conduct a vulnerability assessment under the Act on the Electronic Information Security of State and Local Government Bodies. The requirements for the auditor shall be specified by decree of the President of the SZTFH. The SZTFH shall keep a register of the entities entitled to carry out the audit, as specified in the Decree of the President of the SZTFH. The register shall contain: 1) the auditor's details and the natural person's identification data, telephone number and e-mail address of the auditor's designated contact person; 2) the identification number given when the auditor is registered; 3) the details of the intermediary used by the auditor and the natural person's identity, telephone number and e-mail address of the designated contact person; 4) a document containing the results of the audit.

The auditor shall inform the SAO in writing without delay if he/she identifies, in relation to the electronic information system of the organisation concerned, any fact that seriously jeopardises the continued functioning of the organisation or any circumstances that indicate the commission of a criminal offence, a breach of the law or a serious breach of the internal rules of the organisation concerned or the risk thereof. The auditor shall, to the extent necessary for the conduct of the audit, keep in the audited organisation's possession documents, including personal data and business secrets, received from the audited organisation, necessary for the conduct of the audit, including for the purpose of verifying compliance with the requirements to be verified by the audit, until the audit is completed, and shall not disclose them to any third party.

The auditor is required to set out in the rules the job functions that the persons holding these positions may have access to trade secrets during the audit and the content of these secrets. Staff members involved in the audit are bound by confidentiality obligations

with regard to personal data and business secrets that come to their knowledge during the audit, which shall remain in force for 5 years after termination of employment, and without time limitation with regard to personal data. A cybersecurity audit under this Chapter shall be without prejudice to any certification obligation under other legislation. If the organisation concerned does not comply or does not comply with the legal cybersecurity requirements and related rules of procedure, the NSA shall have the right to warn the organisation concerned to comply with the legal cybersecurity requirements and related rules of procedure, to order the organisation concerned to remedy the security deficiencies discovered or brought to its attention during the audit or inspection or to take the necessary measures to comply with them, setting a time limit, and to prohibit the organisation concerned from any activity that directly jeopardises the fulfilment of the security requirements, taking into account the opinion of the authority that authorised or supervised the organisation's activities.

If, despite the application of the above measures, the organisation concerned fails to comply with the safety requirements and related procedural rules laid down in the legislation, fails to remedy the safety deficiencies or does not cease its activities, the NCA may, after considering all the circumstances of the case, impose a fine as specified in a government decree, which may be repeated in the event of further non-compliance. The SCIO may order that the users of the services provided by the organisation concerned be informed of the potential threat to them or of the expected effects of the preventive measures necessary to counter such threat.

If the auditor fails to comply or does not comply with the cybersecurity requirements and related procedural rules set out in the legislation, the SAO is entitled to: 1) remind you to comply with the legal requirements and related procedural rules; 2) order the remedying of the identified deficiencies or the taking of the necessary measures to comply, setting a time limit; 3) be temporarily suspended from auditing.

For the cybersecurity oversight activities of the CSA, except for budgetary bodies, the entity concerned shall pay a cybersecurity oversight fee at the rate determined by the decree of the President of the CSA pursuant to paragraph 2. The amount of the cybersecurity monitoring fee shall not exceed 0,15 per cent of the net turnover of the organisation listed in Annexes 1 and 2 for the preceding financial year, or, in the absence of turnover, the pro rata temporis share of the turnover for the current year, projected over the whole year. The organisation concerned shall send the information specified in paragraph 1 to the SAEFL within 30 days of the start of its operations for registration.

Unless otherwise provided for by law, data may be transferred from the register referred to in paragraph (1) only to organisations performing official tasks as defined in the Act on the Electronic Information Security of State and Local Government Bodies and to incident management centres. The detailed rules on cooperation and data provision between the SZTFH and the authorities under the Act on the Electronic Information

Security of State and Local Government Bodies shall be laid down by Government decree. If the organisation concerned notifies a change in the data referred to in paragraph (1), the original data shall be deleted from the register by the SZTFH five years after the notification of the change in the data.

8 Reporting cybersecurity incidents

If a security incident has occurred or is imminent in the electronic information system that causes serious disruption or material damage to the operation of the organisation concerned or to the provision of services by it, or causes significant material or non-material damage to other natural or legal persons, the organisation concerned shall immediately notify the incident management centre pursuant to Act L of 2013 on the Electronic Information Security of State and Local Government Bodies, as detailed in the Government Decree. The detailed rules for the handling and technical investigation of security incidents and the notification to the incident management centre shall be specified by Government Decree. If the organisation uses an intermediary for the management of security incidents, the intermediary must have a certificate issued by the SZTFH, as specified in the decree of the President of the SZTFH, attesting to compliance with the rules on the management of security incidents and to the fulfilment of the conditions for the management of security incidents as specified in the decree of the President of the SZTFH. It is of guaranteed importance that these obligations do not affect reporting obligations under other laws.

* * *

From the discussion in this short chapter, it can also be seen that cyber defence results in a forced redesign in the state and local government sector, whereby the legislator's not hidden aim is to outline a predictable course for the organisations concerned, on the one hand, and on the other hand (in justified cases) to ensure the possibility of immediate intervention if the inadequate operation of an organisation in cyberspace is objectionable for reasons of national security.

Chapter II

Cybersecurity in the Republic of Poland

1 Cybersecurity – general issues

Cybersecurity issues in Poland are regulated by the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws of 2022, item 1863), hereinafter referred to as the "NCSA". The Act defines the organisation of the national cybersecurity system, and the duties and obligations of the entities that form its parts, along with the means of exercising supervision and control in the application of the provisions of the Act, and the scope of the Cybersecurity Strategy of the Republic of Poland. The primary objective of this normative act is to regulate issues related to cybersecurity. At the national level, in the first place, the legislator has introduced an elaborated set of very specific concepts and described in detail the system of entities covered by the provisions of this Act (Tyrawa, 2022: 21).

Cybersecurity in the era of information societies has taken on particular importance (Czuryk, 2021: 87). Article 2 (4) of the NCSA defines cybersecurity as the resilience of information systems to actions that compromise the confidentiality, integrity, availability and authenticity of the processed data or related services offered by these systems. In turn, an information system, under Article 2 (14) of the NCSA, means an ICT system together with data in electronic format which are processed therein. Article 3 (3) of the Act of 17 February 2005 on the Computerisation of Business Entities Pursuing Public Tasks (consolidated text, Journal of Laws of 2021, item 2070, as amended) defines an ICT system as a set of cooperating IT devices and software ensuring the processing, storage, as well as the sending and receiving of data via telecommunications networks through telecommunications terminal equipment appropriate for a given type of network. Cybersecurity is a specialised division of security that deals with protecting information systems against threats (Czuryk, 2019: 42), which encompasses the prevention of threats, their anticipation, as well as the mitigation of their consequences, with cyberspace being the venue of their occurrence (Karpiuk, 2021c: 612).

Ensuring digital security is a fundamental task facing the state and its institutions, which is important because of the need to protect both the state and society against cyber threats. The functioning of an information society is based on ICT systems and networks which are sensitive to disruptions affecting their operation. Threats to the IT aspects of a society's functioning increasingly often have far-reaching consequences,

and cyber-attacks can be used as a means of exerting economic and political pressure (Kaczmarek, 2019: 145). ICT systems (especially ones used in executing public tasks) should work uninterruptedly and must be resistant to any actions that may result in decreased quality or interrupt the tasks performed through such systems (Hoffman, Karpiuk, 2022a: 629).

As stipulated in Article 3 of the NCSA, the national cybersecurity system is aimed at ensuring cybersecurity at the national level, including the uninterrupted provision of essential services and digital services, by attaining an adequate level of security of the information systems used to provide these services and ensuring incident handling. The national cybersecurity system should operate as an actual system, i.e., as a set of synchronised elements, both of an institutional and functional nature, within the boundaries of which specific tasks are implemented using the competencies granted to the entities of this system. The system is composed of statutorily designated cybersecurity system entities which should be organised into a certain whole and provided with appropriate resources (Karpiuk, 2021b: 234).

A list of these national cybersecurity system entities is provided in Article 5 of the NCSA, and it includes: 1) operators of essential services; 2) digital service providers; 3) CSIRT MON (the Computer Security Incident Response Team operating at the national level, led by the Minister of National Defence – Article 2 (2) of the NCSA); 4) CSIRT NASK (the Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network National Research Institute – Article 2 (3) of the NCSA); 5) CSIRT GOV (the Computer Security Incident Response Team operating at the national level, led by the Head of the Internal Security Agency – Article 2 (1) of the NCSA); 6) sectoral cybersecurity teams; 7) public finance sector entities (these entities include: a) public authorities, including government administration bodies, state control and law protection bodies, as well as courts and tribunals, b) local government units and their unions, c) metropolitan unions, d) budgetary entities, e) local government budgetary establishments, f) executive agencies, g) budgetary economy institutions, h) the Social Insurance Institution and funds managed by it, and the Agricultural Social Insurance Fund and funds managed by the President of the Agricultural Social Insurance Fund, i) the National Health Fund, j) public higher education institutions, k) the Polish Academy of Sciences and organisational units created by it – Article 9 of the Act of 27 August 2009 on public finance (consolidated text, Journal of Laws of 2022, item 1634, as amended); 8) research institutes; 9) the National Bank of Poland; 10) Bank Gospodarstwa Krajowego; 11) the Office of 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 provincial funds for environmental protection and water management; 15) commercial law partnerships and companies performing public utility tasks (the purpose of performing public utility tasks is to ensure the current and uninterrupted satisfaction of the collective needs of the population by way

of rendering generally available services – Article 1 (2) of the Act of 20 December 1996 on municipal management, consolidated text, Journal of Laws of 2021, item 679, as amended); 16) cybersecurity service providers; 17) authorities competent for cybersecurity; 18) the Single Point of Contact for cybersecurity issues (hereinafter: the Single Point of Contact); 19) the Government Plenipotentiary for Cybersecurity (hereinafter: the Plenipotentiary); and 20) the Committee of Cybersecurity (hereinafter: the Committee). Other entities will not form parts of the national cybersecurity system, but this does not mean that they are exempt from any obligations related to cybersecurity, as they should also take due care of the safety of the ICT systems which they use for their activities or communication purposes. A lack of proper cyberspace surveillance can lead to substantial economic and social damage, including criminal damage. Such damage may also infringe upon the foundations of the state which is composed of its defence and security. Cyber threats significantly influence those two spheres of the state's activity that are the guarantors of its existence.

Ensuring security in cyberspace, both individually and collectively, is a cross-cutting task, the implementation of which rests with several authorities and entities, especially bearing in mind that the national cybersecurity system established by the Polish legislator does not have a centralised character. In particular, the state and public administration must establish appropriate mechanisms, processes and procedures, along with a system that will enable to attain, and continuously increase, the level of cybersecurity in a way that would match the evolving threats. The specific character of cybersecurity means that not only the sovereign powers of a prescriptive or controlling nature are at stake but also those of other nature. The state is obliged to ensure the adequate organisational, human and technical resources necessary to carry out its tasks. The objective awareness of threats, international obligations and national legal regulations, as well as strategic documents – all these require the far-reaching engagement of various actors in this domain (Zdzikot, 2022:45). 45).

2 Operators of essential services

As stipulated in Article 5 (1) of the NCSA, an operator of essential services is an entity designated by the legislator, having its organisational unit in the territory of the Republic of Poland, in respect of which the competent authority for cybersecurity has issued a decision on recognising it as an operator of essential services. The essential service, as defined in Article 2 (16) of the NCSA, is a service that is of key importance for the maintenance of a critical social or economic activity, as mentioned in the list of essential services. Therefore, essential services will be of fundamental importance in the social and economic spheres, as a result of which any disruptions in their provision may adversely affect both the state and society, leading to various crises.

The competent authority for cybersecurity, under Article 5 (2) of the NCSA, issues a decision to recognise an entity as an operator of essential services if 1) that entity

provides an essential service; 2) the provision of that service depends on information systems; 3) the incident would have a major disturbing effect on the provision of an essential service by that operator. The status of an operator of essential services is assigned by way of an administrative decision. All the above conditions should be satisfied jointly for the public administration authority to be able to recognise, in its decision, a given entity as an operator of essential services. A given entity is recognised as an operator of essential services by way of a formal administrative procedure, entailing certain guarantees and ending with a decision (Lebowa, 2022: 103).

The materiality of the disruptive effect of an incident on the provision of an essential service, as a prerequisite for an operator being recognised as an operator of essential services, is determined based on the materiality thresholds of the disruptive effect. The materiality thresholds of the disruptive effect of an incident on the provision of an essential service, and the essential services themselves, are listed in the Regulation of the Council of Ministers of 11September 2018 on the list of essential services and the materiality thresholds of the disruptive effect of an incident on the provision of essential services (Journal of Laws of 2018, item 1806). The thresholds taken into consideration include 1) the number of users dependent on the essential service provided by a specific entity; 2) the dependence of other sectors on the service provided by the entity; 3) the impact that the incident, in terms of scale and duration, could have on economic and social activities, or public security; 4) the market share of the entity providing the essential service; 5) the geographic scope related to the area that could be affected by the incident; 6) the ability of the entity to maintain a sufficient level of the provision of that essential service, taking into account the availability of alternative means of providing it. In turn, the list of essential services covers, *inter alia*, the following: 1) natural gas extraction; 2) oil extraction; 3) lignite extraction; 4) hard coal extraction; 5) copper extraction; 6) the production of electricity; 7) the transmission of electricity; 8) the distribution of electricity; 9) trading in electricity; 10) the storage of electricity; 11) system services, quality services and energy infrastructure management; 12) the production of heat; 13) trading in heat; 14) the transmission of heat; 15) the distribution of heat; 16) the production of liquid fuels; 17) the transmission of crude oil; 18) the transmission of liquid fuels; 19) the storage of crude oil; 20) the handling of crude oil; 21) the storage of liquid fuels; 22) the transhipment of liquid fuels; 23) trading in liquid fuels or trading in liquid fuels with foreign countries; 24) the production of synthetic fuels; 25) the production of gaseous fuels; 26) the transmission of gaseous fuels; 27) trading in gaseous fuels or trading in gaseous fuels with foreign countries; 28) the transmission of gaseous fuels; 29) the distribution of gaseous fuels; 30) the storage of gaseous fuels; 31) liquefaction and regasification of LNG, and importation and offloading; 32) the supply of systems, machinery, equipment, materials, raw materials and provision of services to the energy sector; 33) the production of radiopharmaceuticals; 34) the management of radioactive waste; 35) the maintenance of strategic reserves and stocks of crude oil, petroleum products and natural gas; 36) research and development or technological research for the energy sector; 37) passenger

air transport; 38) cargo air transport; 39) service activities in support of air transport by an airport operator; 40) service activities in support of air transport by an undertaking with the status of a regulated agent; 41) service activities in support of air transport by an undertaking with the status of a ground handling agent; 42) service activities in support of air transport by an air navigation service provider; 43) the construction of train timetables; 44) passenger rail transport; 45) freight rail transport; 46) passenger maritime transport; 47) freight maritime transport; 48) freight inland waterway transport; 49) the management of maritime ports; 50) the operation of maritime passenger and freight transport; 51) service activities in support of maritime transport; 52) vessel traffic monitoring; 53) road management; 54) intelligent transport systems; 55) the acceptance of cash deposits or other repayable funds from customers; 56) granting loans for its own account; 57) the performance of the following bank activities: a) accepting deposits of money payable on demand or on a fixed date, and maintaining accounts for such deposits; b) maintaining other bank accounts; c) granting loans; d) carrying out monetary bank settlements; e) granting cash loans; f) providing payment services and issuing electronic money; g) financial forward transactions, h) purchasing and selling monetary claims, i) performing commissioned activities related to the issue of securities, j) trading in securities, k) providing trust services and issuing means of electronic identification, l) accepting cash deposits and cash withdrawals from payment accounts and conducting all activities necessary for the operation of the account; 58) the performance of activities as provided for a bank by a branch of a foreign bank; 59) the operation of a regulated market or other activities related to organising trading in financial instruments and a commodity exchange; 60) the organisation of an alternative system of trading in financial instruments; 61) the conduction of settlements and transactions in trading in financial instruments; 62) the provision of health care by a medical entity; 63) the commanding of units of the State Medical Rescue System; 64) the management of epidemiological data; 65) the collection and provision of Electronic Medical Records; 66) the marketing and distribution of medicinal products; 67) water treatment; 68) water supply; 69) sewage disposal; 70) sewage treatment; 71) the operation of the Internet traffic exchange point (IXP) in Poland; 72) the maintenance of the top-level domain (TLD) registry. The legislator has, therefore, established a broad list of services classified as essential services. They are of great importance for the state and the fulfilment of the basic needs of society, and their provision must be duly protected. This list was established in the form of a regulation, so each time the Council of Ministers deems that there is a need to expand it, it may issue a relevant normative act of general application.

The recognition of an entity as an operator of essential services is done by way of an administrative decision. The decision resolves the case on its merits, either in whole or in part, or otherwise concludes the case in a given instance, as provided for in Article 104 § 2 of the Act of 14 June 1960 – the Code of Administrative Procedure (consolidated text, Journal of Laws of 2021, item 735 as amended) – hereinafter the "CAP". An administrative decision, as an individual external act addressed to a

specifically designated entity, although it is signed by the authority which issued it, as stated by the Provincial Administrative Court in its judgement of 27 April 2020, II SAB/Wa 478/19 (LEX No. 3058962), does not enter into legal transactions nor does it produce any legal effects before it is properly delivered to its addressees. Expressing a decision towards a party gives rise to a new procedural situation, triggering the possibility of appealing. The rendering or announcement of a decision results in its entering into legal transactions. From that moment, the decision becomes binding on both the public administration authority and the party concerned, following which it brings certain consequences arising from legal provisions. Therefore, the competent authority for ensuring cybersecurity must properly deliver the decision on recognising an operator as an operator of essential services to the party of the procedure.

The decision of the competent authority for cybersecurity must satisfy the requirements envisaged in Article 107 of the Act of 14 June 1960 – the Code of Administrative Procedure (consolidated text, Journal of Laws of 2021, item 735 as amended) – hereinafter the "CAP". Therefore, it should contain 1) the indication of the public administration body; 2) the date of issue; 3) the indication of the party or parties; 4) the citation of the legal basis; 5) the decision; 6) the factual and legal justification; 7) an instruction as to whether, and in what manner, it may be appealed against, as well as about the right to waive the appeal and the consequences thereof; 8) the signature with the name and official position of the employee of the body authorised to issue the decision. The factual justification of the decision should include, in particular, the statement of facts that the authority has considered to have been proven, the evidence on which it has relied and the reasons for which it has denied the credibility and evidential value of other evidence, while the legal justification should include an explanation of the legal basis for the decision, citing the provisions of law. The minimum formal requirements for an administrative decision, according to the standpoint of the Provincial Administrative Court, presented in its judgement of 24 March 2022, II SA/Rz 1493/21 (LEX No. 3341759), contain the identification of the issuing authority and the addressee of the decision, a statement of the merits of the case, and the signature of the issuing person representing the administrative authority.

As stipulated in Article 109 of the CAP, the decision is served on the parties in writing. This can be done orally only in exceptional cases. According to the judgement of the Provincial Administrative Court of 3 June 2022, I SA/Wa 2110/17 (LEX No. 3382567), a decision can be announced to the party orally when this lies in the party's best interest and no legal provision prevents it. Therefore, the authority may use the oral form only when the standpoints of the authority and the party are in agreement, whereas in the event of any divergence of these, it is obliged to conduct the procedure and issue a written decision.

As regards an entity that no longer meets the conditions, the competent authority for cybersecurity, according to Article 5 (6) of the NCSA, issues a decision pronouncing

the expiry of the decision on the recognition as an operator of essential services. In this case, the authority competent for cybersecurity does not act within its administrative discretion, as the legislator has imposed on it the obligation to issue a decision derogating the decision on recognition as an operator of essential services from legal transactions.

Decisions issued by the competent authority for cybersecurity (i.e., decisions on recognition as an operator of essential services and decisions pronouncing the expiry of the decision on recognition as an operator of essential services) are immediately enforceable. This immediate enforceability clause is stipulated in Article 5 (7) of the NCSA. The essence of the immediate enforceability clause, arising from the judgement of the Provincial Administrative Court of 22 April 2021, VII SA/Wa 16/21 (LEX No. 3243429), lies in that it is enforceable even though it is not final. Of note is the fact that the decision becomes immediately enforceable on the date of the written decision or on the date of announcing the oral decision if made immediately enforceable. The authority making the decision immediately enforceable is not authorised to determine when the decision is to be considered enforceable.

The list of operators of essential services, as indicated in Article 7 of the NCSA, is maintained by the minister competent for computerisation. It contains the following elements: 1) the name (business name) of the operator of essential services; 2) the sector, sub-sector and the type of entity; 3) the registered office and address; 4) the tax identification number if assigned; 5) the number in the relevant register if assigned; 6) the name of the essential service, consistent with the list of essential services; 7) the date of commencement of the provision of the essential service; 8) information specifying in which Member States of the European Union the entity has been recognised as an operator of essential services; 9) the date of termination of the provision of the essential service; 10) the date of removal from the list of operators of essential services. The inclusions and removals from the list of operators of essential services are done at the request of the competent authority for cybersecurity, submitted immediately after issuing a decision on recognition as an operator of essential services or a decision pronouncing the expiry of the decision on recognition as an operator of essential services. Any changes to the data contained in the list of operators of essential services also take place at the request of the competent authority for cybersecurity, submitted no later than six months after the changes to such data. The inclusions and removals from the list of operators of essential services, and changes to the data contained in such a list, constitute crucial material and technical acts. As the authority does not issue an administrative decision, the operators of essential services will not have the means of control as those that apply to an administrative act. They will not be allowed to appeal against that act to an administrative court. Data contained in the list of operators of essential services is made available by the minister competent for computerisation to the CSIRT MON, CSIRT NASK and CSIRT GOV, and to the sectoral cybersecurity team, concerning the sector or sub-sector for which it was established, as well as to the

operator of essential services insofar as the data concerns such entity. Data contained in the list of operators of essential services, to the extent necessary for the performance of their statutory tasks, is made available by the minister competent for computerisation, upon request, 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 Public Prosecutor's Office; 10) bodies of the National Fiscal Administration; 11) the Director of the Government Security Centre; 12) the State Protection Service. Given the establishment of the Cyberspace Defence Forces, data contained in the list of operators of essential services as regards the performance of tasks related to security in cyberspace, in the military dimension, should also be provided to that entity. In view of the above, the NCSA should contain adequate solutions taking into consideration the legal status of the Cyberspace Defence Forces.

The legislator imposes a number of obligations on the operator of essential services as an entity performing important tasks from the point of view of cybersecurity, including the obligation under Article 8 of the NCSA to implement a security management system in the information system used to provide the essential service, which is expected to ensure: 1) the conduction of a systematic estimation and management of the risk of an incident; 2) the implementation of technical and organisational measures that are appropriate and proportionate to the estimated risk, taking into account the current state of the art, including: a) maintenance and safe operation of the information system, b) physical and environmental safety, taking into account access control, c) security and continuity of the supply of services which are fundamental to the provision of an essential service, d) the implementation, documentation and maintenance of action plans enabling the continuous and uninterrupted provision of the essential service and ensuring confidentiality, integrity, availability and authenticity of information, e) the continuous monitoring of the information system used for the provision of the essential service; 3) the collection of information on cybersecurity threats and vulnerabilities to incidents, identified within the information system used to provide the essential service; 4) incident management; 5) the application of measures to prevent and limit the impact of incidents on the security of the information system used to provide the essential service, including: a) the use of mechanisms to ensure the confidentiality, integrity, availability and authenticity of data processed in the information system, b) care for software updates, c) protection against unauthorised modification in the information system, d) immediate action upon perceived vulnerabilities or cybersecurity threats; 6) the use of communication means to enable proper and secure communication within the national cybersecurity system. Cybersecurity management is an important security element aimed at countering threats emerging in cyberspace. Operators of essential services are also involved in the cybersecurity management process and must manage their activities accordingly, not only in terms of the business activities they perform

using the information system but also from a broader perspective – that of the national cybersecurity system.

The operator of essential services: 1) appoints the person responsible for maintaining contact with entities of the national cybersecurity system; 2) ensures that users of essential services have access to knowledge to better understand cybersecurity threats and apply effective ways to protect themselves against these threats, in the scope related to the essential service provided, in particular by publishing information on this subject matter on its website; 3) provides the competent authority for cybersecurity with information specifying in which Member States of the European Union the entity has been recognised as an operator of essential services and the termination date of the essential service, no later than three months after the change in such data. These obligations arise from Article 9 of the NCSA. Cooperation within the national cybersecurity system is an important aspect in the field of cybersecurity protection. This cooperation is conducted, *inter alia*, through the exchange of information, in connection with which the legislator imposes the obligation to appoint a contact person for national entities to stay informed on the threats emerging in cyberspace that have a significant impact on the operation of information systems.

Operators of essential services develop, apply and update documentation regarding the cybersecurity of the information system used to provide the essential service. They are also obliged to exercise supervision over that documentation, enabling: 1) the accessibility of documents only to authorised persons in line with the tasks assigned to them; 2) the protection of documents against misuse or loss of integrity; 3) the marking of successive versions of documents to identify changes made to them. This obligation arises from Article 10 of the NCSA. However, it does not apply to the operators of essential services that are owners, owner-like possessors or lessees of the facilities, installations, devices or services which comprise critical infrastructure, if they have an approved critical infrastructure protection plan taking into account the documentation regarding the cybersecurity of the information system used to provide the essential service.

Critical infrastructure resources and their protection occupy a major place in the domain of crisis management. In turn, crisis management is one of the underlying elements of the national security system (Czuryk, Dunaj, Karpiuk, Prokop, 2016: 9). Owners, owner-like possessors or lessees of the facilities, installations, devices or services which comprise critical infrastructure – under Article 6 (5) of the Act of 26 April 2007 on crisis management (consolidated text, Journal of Laws of 2022, item 261 as amended) – are obliged to protect them, in particular by preparing and implementing, in line with any anticipated threats, critical infrastructure protection plans, and maintaining their reserve systems ensuring security and continual functioning of this infrastructure until it is fully restored. The structural elements of the critical infrastructure protection plan are defined in § 2 of the Regulation of the Council of Ministers of 30 April 2010 on critical

infrastructure protection plans (Journal of Laws of 2010, No. 83, item 542), including: 1) general data: a) including the name and location of the critical infrastructure, b) identifying the critical infrastructure operator, c) identifying the manager of the company acting on behalf of the critical infrastructure operator, d) including information on the person responsible for maintaining contact with entities competent for the protection of critical infrastructure, e) including the name of the person drawing up the plan; 2) critical infrastructure data including: a) characteristics and basic technical parameters, b) a map showing the location of the facility, installation or system, c) functional links to other facilities, installations, equipment or services; 3) characteristics of: a) threats to critical infrastructure and an assessment of the risk of their occurrence, together with foreseeable scenarios for the development of events, b) the dependence of critical infrastructure on other critical infrastructure systems and the potential for disruption as a result of disruptions to other critical infrastructure systems, c) own resources that may be used for the protection of critical infrastructure, d) resources of locally competent authorities which may be used for the protection of critical infrastructure; 4) essential variants for: a) acting in the event of a threat or disruption to critical infrastructure, b) ensuring the continual functioning of critical infrastructure, c) restoring critical infrastructure; 5) principles of cooperation with locally competent: a) crisis management centres, b) public administration authorities. The critical infrastructure protection plan drawn up by the operator of essential services should also include documentation regarding the cybersecurity of the information systems used to provide the essential services. Countering threats emerging in cyberspace, including cyber terrorism, will be possible by maintaining a high level of security of the information and communication systems which are essential for the proper functioning of the state, the information and communication systems of public administration authorities or information and communication networks included in the uniform list of critical infrastructure facilities, installations, devices and services, as well as the information and communication systems of owners, owner-like possessors and lessees of critical infrastructure facilities, installations or devices, and data processed with the use of such systems (Karpiuk, 2022c: 77).

As stipulated in Article 11 (1) of the NCSA, operators of essential services: 1) ensure incident handling; 2) provide access to information on registered incidents to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams, to the extent necessary for the performance of its tasks; 3) classify incidents as serious based on thresholds for considering incidents as serious; 4) report serious incidents immediately, but in any case not later than within 24 hours from the moment of detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams; 5) cooperate during the handling of serious or critical incidents with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams by providing any necessary data, including personal data; 6) remove the vulnerabilities that have led or could have led to major, significant or critical incidents, and inform the competent authority for cybersecurity of their removal. Operators of

essential services are, therefore, obliged to take measures both to enable the detection of cyber threats and their neutralisation and to mitigate their consequences.

Article 13 (1) of the NCSA indicates the possibility for operators of essential services to provide information to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams, regarding 1) other incidents; 2) cyber threats; 3) risk estimation; 4) vulnerabilities; 5) technologies used. The information collected by the relevant CSIRT team is not only an objective in itself but also a decision-making tool, as the analyses undertaken based on such information can serve the purpose of cybersecurity prevention (Włodyka, 2022: 211).

Article 15 (1) of the NCSA imposes an obligation on operators of essential services to conduct a security audit of the information systems used to provide the essential services at least once every two years. The audit is a source of information on the operation of the information system, its resilience to cyber threats, as well as the ability to provide quality essential services, and disruptions to its operation. Based on the audit report, the operator of essential services can take appropriate preventive measures if these are required given the provision of essential services through the information system.

The audit is seen as a form of support for an entity in terms of managing the tasks it performs. One of the objectives of the audit is to provide the audited entity's manager with information on whether all processes are conducted following the principle of legality and the accepted arrangements. Undoubtedly, the effectiveness associated with the conduction of an internal audit largely depends on the knowledge, competence and efficiency of the auditor (Romaniuk, 2022: 192).

Authorities competent for cybersecurity supervise and inspect the performance of obligations imposed on operators of essential services arising from the NCSA which concern combating cyber threats and reporting serious incidents. As regards entrepreneurs with operator of essential services status – as stipulated in Article 47 of the Act of 6 March 2018 – the Enterprise Law (consolidated text, Journal of Laws of 2021, item 162 as amended) – inspections are planned and conducted following the prior analysis of the likelihood of a breach of law in connection with carrying out business activities. The analysis includes the identification of the subject and object areas where the risk of infringement is the greatest. However, this does not apply to instances where the inspection authority reasonably suspects: 1) a threat to life or health; 2) the commission of a crime or a petty offence; 3) the commission of a fiscal crime or petty offence; 4) another breach of a legal prohibition or failure to comply with a legal obligation – in connection with carrying out the business activities which are being inspected. Because of the great significance of ICT systems, both for the economy and the public sphere, the state must be in possession of adequate tools to combat cyber-attacks, especially those relevant to its operation. In this respect, great importance must

be attached to surveillance and inspection. It is the purpose of both supervision and inspection to prevent unwanted incidents in cyberspace and, therefore, to ensure that cybersecurity is at an adequate level to allow the uninterrupted performance of tasks. The ideal status, i.e., a lack of any disruptions, is not achievable. So, what is at stake is the level of cybersecurity that allows the needs which arise to be met uninterruptedly, while maintaining appropriate quality standards, offering an adequate availability of services, and ensuring the optimum cost of service provision (Czuryk, 2022c: 112).

3 Digital service providers

The definition of digital service providers is contained in Article 17 (1) of the NCSA which stipulates that these are legal persons or organisational units without legal personality having their registered office or management board in the territory of the Republic of Poland, or acting via a representative having its organisational unit in the territory of the Republic of Poland, providing digital services, including services rendered by electronic means, except for micro- and small enterprises. Micro- and small enterprises are defined in Article 7 of the Act of 6 March 2018 – the Enterprise Law (consolidated text, Journal of Laws of 2021, item 162, as amended). A micro-enterprise is an enterprise which, in at least one of the last two financial years, jointly fulfilled the following conditions: 1) employed less than 10 employees on an average annual basis; 2) achieved an annual net turnover from the sales of goods, products and services as well as from financial operations not exceeding the PLN equivalent of EUR 2 million, or the sum of the assets of its balance sheet drawn up at the end of one of those years did not exceed the PLN equivalent of EUR 2 million. In turn, a small enterprise is an enterprise which, in at least one of the last two financial years, jointly fulfilled the following conditions: 1) employed less than 50 employees on an average annual basis; 2) achieved an annual net turnover from the sales of goods, products and services as well as from financial operations not exceeding the PLN equivalent of EUR 10 million, or the sum of the assets of its balance sheet drawn up at the end of one of those years did not exceed the PLN equivalent of EUR 10 million, and which is not a micro-enterprise.

Pursuant to Article 17 (2) of the NCSA, the digital service provider takes appropriate and proportionate technical and organisational measures to manage the risks to which the information systems used to provide the digital service are exposed. These measures should ensure a level of cybersecurity appropriate to the risks involved and should take into account: 1) the security of information systems and facilities; 2) incident handling; 3) management of the provider's business continuity for the provision of the digital service; 4) monitoring, auditing and testing; 5) the state of the art, including compliance with international standards. An important responsibility imposed on the digital service provider is to manage the risks associated with the use of the information system to provide the digital service. This management is to protect against disruptions to the information system, to ensure the continuity of its operation and the high quality of

services. An audit is an element of risk management. Therefore, it is important to draw information from the audit which will facilitate the decision-making process connected with ensuring the cybersecurity of the provision of digital services.

Article 18 (1) of the NCSA imposes the following obligations on digital service providers: 1) carry out activities enabling the detection, recording, analysis and classification of incidents; 2) provide, to the extent necessary, access to information for the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams on incidents classified as critical by the relevant CSIRT MON, CSIRT NASK or CSIRT GOV teams; 3) classify the incident as significant; 4) report the significant incident promptly, no later than within 24 hours of detection, to the relevant CSIRT MON, CSIRT NASK or CSIRT GOV team; 5) ensure the handling of a serious incident and a critical incident in cooperation with the relevant CSIRT MON, CSIRT NASK or CSIRT GOV team, providing the necessary data, including personal data; 6) remove the vulnerabilities that have led or could have led to serious, significant or critical incidents; 7) provide to the operator of essential services that renders the essential service through that digital service provider information regarding an incident affecting the continuity of the essential service of that operator. These obligations are intended to ensure the level of cybersecurity enabling the provider's uninterrupted provision of digital services. Their implementation will be possible not only through adequate financial resources but also through the application of appropriate organisational and technical measures.

Digital services are listed in Annex 2 to the NCSA, including 1) an online trading platform – a service that enables consumers or traders to enter into contracts electronically with traders on the website of the trading platform or on the website of the trader who uses the services provided by the online trading platform; 2) a cloud computing service – a service that enables access to a scalable and flexible set of computing resources for shared use by multiple users; 3) a web search engine – a service that allows users to search all web pages or sites in a particular language based on a query by entering a keyword, a phrase or another element, yielding links that refer to information related to the query.

4 Tasks of Computer Security Incident Response Teams

CSIRT MON, CSIRT NASK and CSIRT GOV cooperate amongst themselves, along with the authorities competent for ensuring cybersecurity, the minister competent for computerisation and the Plenipotentiary, ensuring a coherent and complete risk management system at the national level, carrying out tasks to counteract cybersecurity threats of a cross-sectoral and cross-border nature, as well as ensuring coordination of the handling of reported incidents. These tasks are provided for in Article 26 (1) of the NCSA. CSIRT teams can also provide support in handling incidents. However, the legislator indicates the possibility of providing such support, rather than an obligation to do so (Karpiuk, 2020: 63).

The tasks of CSIRT teams are defined in Article 26 (3) of the NCSA, which indicates that they include: 1) monitoring cybersecurity threats and incidents at the national level; 2) estimating risks related to any identified cybersecurity threats and incidents, including the performance of dynamic risk analysis; 3) providing information concerning incidents and risks to entities within the national cybersecurity system; 4) issuing alerts on identified cybersecurity threats; 5) responding to reported incidents; 6) classifying incidents, including serious and significant incidents, as critical incidents, and coordinating the process of critical incident handling; 7) reclassifying serious and significant incidents; 8) providing the competent CSIRT MON, CSIRT NASK or CSIRT GOV teams with technical information on incidents the handling of which needs to be coordinated by way of CSIRT cooperation; 9) performing, in justified cases, device or software testing to identify any vulnerabilities which could be used to threaten the integrity, confidentiality, accountability, authenticity or availability of processed data, which may affect public safety or a vital interest of national security, as well as submitting applications regarding recommendations for entities within the national cybersecurity system on the use of device and software, especially as regards their impact on public safety or a vital interest of national security; 10) cooperating with sectoral cybersecurity teams in the field of the coordination of serious incident handling, including incidents concerning two or more EU Member States, and critical incidents, as well as the exchange of information enabling the counteracting of threats to cybersecurity; 11) providing to, and receiving from, other countries, including EU Member States, information on serious and significant incidents concerning two or more EU Member States, and submitting to the Single Point of Contact notifications of serious and significant incidents concerning two or more EU Member States; 12) providing, by 30 May each year, to the Single Point of Contact a list of serious incidents reported in the preceding calendar year by operators of essential services affecting the continuity of essential services provided by them in the Republic of Poland and the continuity of essential services provided in EU Member States, as well as a list of significant incidents reported in the preceding calendar year by digital service providers, including those concerning two or more EU Member States; 13) preparing and submitting jointly to the minister competent for computerisation the part of the Report on threats to national security regarding cybersecurity; 14) ensuring analytical and R&D infrastructure, which in particular a) conducts advanced malware analyses and vulnerability analyses, b) monitors cybersecurity threat indicators, c) develops tools and methods for detecting and combating cybersecurity threats, d) conducts analyses and develops standards, recommendations and good practices as regards cybersecurity, e) supports entities within the national cybersecurity system in capacity building in the sphere of cybersecurity, f) carries out activities to increase awareness of cybersecurity, g) cooperates in the scope of educational solutions in relation to cybersecurity; 15) ensuring the possibility to report and provide information, as well as provides access to and operates the means of communication that makes it possible to deliver notifications; 16) participating in the CSIRT network comprising representatives of the CSIRTs in EU

Member States, the CSIRT responsible for the institutions of the European Union, the European Commission and the European Union Agency for Cybersecurity (ENISA). These are general tasks assigned to individual CSIRT teams performed within the scope of their competence. The broad scope of these tasks demonstrates the importance of CSIRT teams in the national cybersecurity system. They are the basic link of this system. The legislator also distinguishes the specific tasks of Computer Security Incident Response Teams.

The tasks of CSIRT MON, under Article 26 (5) of the NCSA, include the coordination of the handling of incidents reported by: 1) entities subordinate to, or supervised by, the Minister of National Defence, including entities whose information and communication systems or networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure; 2) entrepreneurs performing tasks for the Polish Armed Forces. Under Article 648 (1) of the Act of 11 March 2022 on Homeland Defence (Journal of Laws of 2022, item 655 as amended), - hereinafter: the HDA - the tasks carried out by entrepreneurs for the Polish Armed Forces include: 1) manufacturing, carrying out repairs or providing services for the Polish Armed Forces under conditions of threat to state security or in times of war; 2) maintaining, in peacetime, manufacturing, repair or service capacities necessary to perform the above tasks; 3) militarisation; 4) the protection of facilities particularly important for state security and defence; 5) other tasks performed for the Polish Armed Forces and allied troops.

The tasks of CSIRT NASK, as per Article 26 (6) of the NCSA, include: 1) the coordination of the handling of incidents reported by: a) public finance sector units (local government units and their unions, metropolitan unions, budgetary entities, local government budgetary establishments, executive agencies, budgetary economy institutions, public higher education institutions, the Polish Academy of Sciences and organisational units created by it), b) units subordinate to government administration bodies or supervised by them (except for units subordinate to the Prime Minister or supervised by him), c) research institutes, d) the Office of Technical Inspection, e) the Polish Air Navigation Services Agency, f) the Polish Centre for Accreditation, g) the National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management, h) commercial law partnerships and companies performing public utility tasks, i) digital service providers, j) the operators of essential services, k) other entities, and l) individuals; 2) the creation and provision of tools for voluntary cooperation and the exchange of information on cybersecurity threats and incidents; 3) the provision of a telephone line or Internet service operating in the field of reporting and the analysis of cases of the distribution, dissemination or transmission of child pornography through information and communication technologies.

The tasks of the CSIRT GOV, under Article 26 (7) of the NCSA, include the coordination of the handling of incidents reported by: 1) selected public-finance entities (government administration authorities, state control and law protection bodies, courts and tribunals); 2) the Social Insurance Institution and funds managed by it, the Agricultural Social Insurance Fund and funds managed by the President of the Agricultural Social Insurance Fund; 3) the National Health Fund; 4) entities subordinate to or supervised by the Prime Minister; 5) the National Bank of Poland, 6) the National Economy Development Bank, 7) other entities whose information and communication systems or networks are included in the uniform list of facilities, installations, devices, and services which comprise critical infrastructure.

CSIRT MON, CSIRT NASK or CSIRT GOV, whoever has received an incident notification, but is not responsible for coordinating its handling, shall immediately forward this report to the competent CSIRT team, along with the information received. This principle is introduced in Article 26 (8) of the NCSA. This makes it possible to counteract cybersecurity threats, even if an incident has been reported to the wrong CSIRT team, in which case it is required to forward such an incident notification, along with the information it has, to the competent CSIRT team, which can perform any appropriate tasks.

Further tasks of CSIRT GOV and CSIRT MON are defined in Article 27 of the NCSA. CSIRT GOV is competent for terrorist incidents. A terrorist incident should be understood as a situation where there is the suspicion that it has occurred as a result of a terrorist offence, or the threat of such an offence – Article 2 (7) of the Act of 10 June 2016 on Measures to Combat Terrorism (consolidated text: Journal of Laws of 2021, item 2234, as amended). Pursuant to Article 115 § 20 of the Act of 6 June 1997 – the Penal Code (consolidated text: Journal of Laws of 2022, item 1138 as amended), a terrorist offence is a prohibited act subject to imprisonment with the upper sentence limit of at least five years, committed with the aim of 1) seriously intimidating a population, 2) unduly compelling the public authorities of the Republic of Poland or another state Government or international organisation to perform or abstain from performing an act, 3) seriously destabilising or destroying the structures or the economy of the Republic of Poland, another state or an international organisation - as well as a threat to commit such an act. CSIRT MON is competent for handling terrorist incidents which compromise the security of the national defence potential, the Polish Armed Forces and organisational units of the Ministry of National Defence (Article 5 (1) (2a) of the Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service, consolidated text: Journal of Laws of 2022, item 502, as amended).

CSIRT MON, CSIRT NASK and CSIRT GOV, under Article 35 (1) of the NCSA, provide each other with information on a critical incident (a critical incident is an incident leading to significant damage to public safety or public order, international interests, economic interests, public institutions' activities, civil rights and freedoms,

and/or human health and life, as classified by the competent CSIRT MON, CSIRT NASK or CSIRT GOV teams – Article 2 (6) of the NCSA) and inform the Government Centre for Security of the incident.

CSIRT teams in the national cybersecurity system play a supporting role, with expertise in handling incidents. As the undertaken analytical activities and the ability to exchange information highly contribute to the protection of cybersecurity, they rank highly in this system (Kostrubiec, 2022b: 34).

5 Competent authorities for cybersecurity

The catalogue of competent authorities for cybersecurity is included in Article 41 of the NCSA, according to which they are: 1) for the energy sector – the minister competent for energy; 2) for the transport sector, excluding the water transport subsector – the minister competent for transport; 3) for the water transport subsector – the minister competent for the maritime economy and the minister competent for inland navigation; 4) for the banking sector and financial market infrastructure sector – the Polish Financial Supervision Authority (KNF); 5) for the healthcare sector, excluding entities subordinate to and supervised by the Minister of National Defence – the minister competent for health; 6) for the healthcare sector comprising entities subordinate to and supervised by the Minister of National 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, excluding entities subordinate to and supervised by the Minister of National Defence – the minister competent for computerisation; 9) for the digital infrastructure sector comprising entities subordinate to and supervised by the Minister of National Defence - the Ministry of National Defence; 10) for digital service providers, excluding entities subordinate to and supervised by the Minister of National Defence – the minister competent for computerisation; 11) for digital service providers comprising entities subordinate to and supervised by the Minister of National Defence – the Minister of National Defence. The catalogue of authorities listed in Article 41 of the NCSA is closed, so other authorities, even those performing cybersecurity tasks, will not have the status of competent authorities for cybersecurity to which the legislator has assigned specific tasks.

The competent authority for cybersecurity, according to Article 42 of the NCSA, performs the following tasks: 1) it performs analyses, on an ongoing basis, of entities in a given sector or sub-sector in terms of recognising them either as an operator of essential services or identifying non-compliance with the conditions qualifying a given entity as an operator of essential services; 2) issues decisions recognising a given entity as an operator of essential services, or decisions confirming the expiration of the decision recognising a given entity as an operator of essential services; 3) immediately after issuing a decision recognising a given entity as an operator of essential services or

a decision confirming the expiration of the decision recognising a given entity as an operator of essential services, it submits applications to the minister competent for computerisation to enter that entity in to the list of operators of essential services or to remove them from that list; 4) submits applications to change data in the list of operators of essential services, not later than within six months from the change of these data; 5) prepares, in cooperation with CSIRT NASK, CSIRT GOV, CSIRT MON and sectoral cybersecurity teams, recommendations on actions aimed at strengthening cybersecurity, including sectoral guidelines on reporting incidents; 6) monitors the application of the provisions of the Act by operators of essential services and digital service providers; 7) requires operators of essential services or digital service providers, at the request of CSIRT NASK, CSIRT GOV or CSIRT MON, to remove, within the prescribed period, the vulnerabilities that led or could lead to a serious, significant or critical incident; 8) conducts inspections of operators of essential services and digital service providers; 9) may cooperate with the competent authorities of the EU Member States via the Single Point of Contact; 10) processes information, including personal data, about the essential and digital services being provided and the operators of essential services or digital service providers to the extent necessary to perform the tasks provided for in the Act; 11) participates in cybersecurity exercises organised in the Republic of Poland or in the European Union.

Among the authorities competent for cybersecurity the most important ones are the Minister of National Defence and the minister competent for computerisation. The scope of action of the Minister of Defence in peacetime includes managing all activities of the Polish Armed Forces, which also applies to their activities related to ensuring security in cyberspace in the military dimension (Karpiuk, 2022b:87). The Minister of National Defence is responsible for 1) the cooperation of the Polish Armed Forces with the relevant authorities of the North Atlantic Treaty Organisation, the European Union and other international organisations, in the field of national defence and, more specifically, cybersecurity; 2) ensuring the capacities of the Polish Armed Forces, in domestic, alliance and coalition relations, for conducting military operations in the event of a threat to cybersecurity triggering the need to take defensive measures; 3) developing the abilities of the Polish Armed Forces as regards the provision of cybersecurity by organising specialised training; 4) acquiring and developing tools to be used by the Polish Armed Forces for capacity-building as regards the provision of cybersecurity; 5) managing activities related to incident handling under martial law; 6) assessing the impact of incidents on the state's defence system; 7) assessing threats to cybersecurity under martial law and presenting proposals regarding defensive measures to competent authorities; 8) coordinating, in cooperation with the minister competent for internal affairs and the minister competent for computerisation, the performance of duties by government administration and local government authorities under martial law, regarding defensive measures in the event of a threat to cybersecurity. This responsibility is provided for in Article 51 of the NCSA. It entails matters falling within

the defence sphere involving cyberspace, which is of great importance for maintaining the readiness of the Polish Armed Forces, including the Cyberspace Defence Forces.

The minister competent for computerisation is responsible for 1) monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, and associated action plans; 2) recommending the spheres of cooperation with the private sector in order to increase the cybersecurity of the Republic of Poland; 3) preparing annual reports regarding a) serious incidents reported by any operators of essential services affecting the continuity of provision of their essential services in the Republic of Poland and in the Member States of the European Union; b) significant incidents reported by digital service providers, including those involving two or more European Union Member States; 4) conducting informational activities on good practices, educational programmes, campaigns, and training, to expand knowledge and to build awareness of cybersecurity, including the safe use of the Internet by various categories of users; 5) collecting information on serious incidents which concerns, or has been provided by, another Member State of the European Union; 6) providing information and good practices related to the notification of serious incidents by the operators of essential services, and significant incidents by digital service providers, obtained from the Cooperation Group, including a) incident-management procedures, b) risk-management procedures, c) the classification of information, risks, and incidents. The aforementioned responsibility of the minister competent for computerisation is defined in Article 45 of the NCSA and concerns cyberspace security in the civilian dimension.

The minister competent for computerisation runs the Single Point of Contact, whose tasks are listed in Article 48 of the NCSA, and include: 1) receiving notifications of serious or significant incidents involving two or more EU Member States from single points of contact in other EU Member States and forwarding such notifications to CSIRT MON, CSIRT NASK, CSIRT GOV or sectoral cybersecurity teams; 2) forwarding, at the request of a relevant CSIRT MON, CSIRT NASK, or CSIRT GOV team, notifications of serious or significant incidents involving two or more EU Member States to single points of contact in other EU Member States; 3) ensuring the representation of the Republic of Poland in the Cooperation Group; 4) ensuring cooperation with the European Commission in the sphere of cybersecurity; 5) coordinating cooperation between competent authorities for cybersecurity and public authorities in Poland with relevant authorities in other EU Member States; 6) ensuring the exchange of information for the benefit of the Cooperation Group, and the CSIRT Network.

Ensuring cyberspace security in the civilian dimension is within the scope of duties of the minister competent for computerisation. However, not all matters in this area will fall within the competence of this minister, as the President of the Council of Ministers may entrust certain entities with the implementation of tasks arising from, among others, the sphere of digital innovation, the development of an information society or

counteracting digital exclusion. The entrustment of these tasks is intended to support the development of a digital society, shape the digital awareness of citizens, and raise awareness of cyber threats, hence fostering the dissemination of information about the need to conduct such activity −with the use of communication and information systems − that respects the principles of cybersecurity (Karpiuk, 2022a: 18).

6 Cybersecurity Strategy of the Republic of Poland

One of the tasks of public administration bodies is planning and preparing various types of plans, strategies, and programmes. These documents often have to take into account cybersecurity issues to ensure the efficient performance of public tasks that require protection against cyber threats. Planning, including actions related to security in cyberspace, allows the performance of coordinated action to enable the proper, timely and smooth implementation of the objectives set for public administration authorities in an organised and continuous manner, including the engagement of multiple actors in the process (Karpiuk, 2021a: 46).

The Cybersecurity Strategy of the Republic of Poland (the Strategy) is adopted by the Council of Ministers. The legal form of this document is a resolution, a legal act that is binding internally, but not externally. Therefore, it does not impose any obligations on external entities.

The scope of the Strategy is defined in Article 69 of the NCSA. The Strategy sets out strategic objectives and political and regulatory measures to ensure a high level of cybersecurity. In particular, it includes: 1) objectives and priorities related to cybersecurity; 2) entities involved in the implementation and execution of the Strategy; 3) measures applied to achieve the objectives of the Strategy; 4) the identification of response and recovery measures, including principles of cooperation between the public and private sectors; 5) the approach to risk assessment; 6) activities related to cybersecurity education, information and training programmes; 7) activities related to research and development plans in the area of cybersecurity. It is adopted for a period of five years with the possibility to introduce amendments during the time.

The Cybersecurity Strategy of the Republic of Poland for 2019-2024 assumes, as its main objective, increasing the level of resilience to cyber threats and the level of protection of information in the public, military, and private sectors, as well as promoting awareness and good practices to enable citizens to better protect their data. The detailed objectives include 1) the development of the national cybersecurity system; 2) increasing the level of resilience of information systems of both the public administration and the private sector to effectively prevent and respond to incidents; 3) enhancing domestic capabilities in the area of cybersecurity; 4) increasing public awareness and competences in the area of cybersecurity; 5) building a strong international position of the Republic of Poland in the cybersecurity domain. It rightly

underlines that social and economic development is increasingly dependent on fast and free access to information and its use in the sectors of management, production, and services, as well as the public sector. At the same time, the dynamic development of information systems is conducive to the development of the national economy, in particular in the areas of communication, trade, transport or finances. Digital technologies that make up cyberspace shape social relations, while the services provided on the Internet have become a tool for influencing the behaviour of social groups as well as politics.

7 Cybersecurity Fund

As stipulated in Article 2 of the Act of 2 December 2021 on Special Rules of Remuneration for Individuals Performing Cybersecurity Tasks (Journal of Laws of 2021, item 2333, as amended) – hereinafter referred to as the ASRR - the purpose of the Cybersecurity Fund is to support activities aimed at ensuring the security of ICT systems against cyber threats. The Fund is administered by the minister competent for computerisation. The resources of the Cybersecurity Fund are allocated for the provision of ICT services and related costs. The Director of the Research and Academic Computer Network – The National Research Institute may, in consultation with the minister competent for computerisation, allocate part of the funds from the financial plan of that institute, including the net profits of the Research and Academic Computer Network – the National Research Institute for the previous financial year, to the fund. Its operating costs are financed from the State budget, from the part available to the minister competent for computerisation. Financing from the fund's resources may be requested for tasks aimed at ensuring the security of information and communication systems against cyber threats. Support is granted based on an agreement made between the minister competent for computerisation and the applicant who must be an entity implementing tasks in the field of cybersecurity. The minister competent for computerisation may, in consultation with the minister competent for public finance, transfer part of the resources from the Broadband Fund to the Cybersecurity Fund. The Broadband Fund is administered by the minister competent for computerisation and the resources are allocated for 1) activities supporting the development of high-speed telecommunications networks by subsidising or granting loans for the construction or reconstruction of these networks and the construction of telecommunications connections to the end user's location; 2) activities aimed at stimulating end-user demand for broadband Internet services by subsidising the purchase of telecommunications services, multimedia devices, as well as the organisation of, or participation in, training courses to develop digital competencies. These funds may also constitute revenue for the Cybersecurity Fund – Article 16a of the Act of 7 May 2010 on the Support for Telecommunications Services (consolidated text, Journal of Laws of 2022, item 884, as amended).

The Cybersecurity Fund is a state earmarked fund. As stipulated in Article 29 of the Act of 27 August 2009 on public finances (consolidated text, Journal of Laws of 2022, item 1634 as amended), state earmarked funds are established based on an act and their revenues are derived from public funds. They incur costs for the implementation of specific public tasks. State earmarked funds do not have legal personality, but have a separate bank account administered by the minister indicated in the law creating a given fund or another entity indicated in that law.

In order to receive support from the Cybersecurity Fund, as stipulated in Article 3 (1) of the ASRR, the relevant entity must submit an application to the minister competent for computerisation, containing: 1) a detailed description of the cybersecurity tasks along with the number of persons performing a given task; 2) a statement by the head of the applying entity on the fulfilment of the requirements stipulated by law; 3) an indication of the maximum amount of the projected costs related to the granting of the ICT benefit; 4) the expected date of receipt of funds from the Cybersecurity Fund for the ICT benefit.

Persons entitled to receive an ICT benefit (an allowance for work and, in the case of officers and professional soldiers, consideration in cash) are defined in Article 5 of the ASRR. These include persons performing tasks: 1) in the bodies and entities listed in the NCSA: (a) in CSIRT teams, (b) in competent authorities for ensuring cybersecurity, (c) in sectoral cybersecurity teams, (d) for the Government Plenipotentiary for Cybersecurity; 2) in respect of ensuring cybersecurity in: (a) the Internal Security Agency, (b) the Intelligence Agency, (c) the Central Anti-Corruption Bureau, (d) organisational units subordinate to the Prime Minister or ministers, (e) the Chancellery of the Prime Minister and at agencies supporting ministers, (f) the Chancellery of the President of the Republic of Poland, g) the Chancellery of the Sejm, h) the Chancellery of the Senate, i) the Police, j) the Public Prosecutor's Office, k) the Military Counterintelligence Service, l) the Military Intelligence Service, m) the Border Guard, n) the State Protection Service.

Under Article 7 of the ASRR, the amount of the remuneration for work with bonuses or salary with bonuses, including the ICT benefit, may not exceed twenty-one times the base amount for civil servants set out in the Budget Act. The ICT benefit is granted annually for the period of performance of cybersecurity tasks. The decision regarding its granting or withdrawal is made by the head of the entity in which individuals performing cybersecurity tasks are employed or serve as officers or professional soldiers. An individual performing cybersecurity tasks loses the entitlement to the granted ICT benefit in the event of 1) being punished with a penalty for a breach of duties or disciplinary action; 2) being unjustifiably absent from work for at least two days; 3) reporting for work or service under the influence of alcohol or intoxicants; 4) consuming alcohol or using intoxicants during work or service; 5) leaving a place of work or service without justification.

Detailed cybersecurity tasks for the performance of which the ICT benefit is due are set out in the Regulation of the Council of Ministers of 19 January 2022 on the amount of the ICT benefit for individuals performing cybersecurity tasks (Journal of Laws of 2022, item 131), including: 1) the active identification of cybersecurity threats; 2) malware analysis; 3) the testing of security, vulnerability, hardware, and software; 4) the assessment of information system security, including penetration tests and security audits; 5) conducting specialised cybersecurity analyses and detecting new vulnerabilities; 6) developing specialised technical tools to support cybersecurity tasks; 7) managing a unit or organisational unit dedicated to the performance of cybersecurity tasks; 8) undertaking preventive measures to enhance cybersecurity; 9) conducting advanced tasks in the area of active defence of information systems; 10) advanced incident handling; 11) post-intrusion analysis; 12) the research into, and evaluation of, the security of ICT solutions; 13) designing, building and maintaining incident monitoring and detection systems and supporting the operation of the Security Operations Centre (SOC) as well as the Computer Security Incident Response Team (CSIRT); 14) data correlation, conducting analyses or creating situational maps; 15) monitoring cybersecurity threats and incidents at the domestic level; 16) conducting analyses of serious incidents, establishing links between incidents and developing conclusions; 17) receiving notifications and handling major incidents; 18) responding to and classifying incidents; 19) performing analyses and management tasks when responding to detected hardware and software vulnerabilities; 20) coordination when handling reported incidents; 21) the handling of notifications and content analysis of cases of the distribution, dissemination or transmission of child pornography via ICT networks; 22) specialised tasks implemented as part of the SOC or Network Operations Centre (NOC) including: security monitoring, identification and initial incident handling; 23) the estimation of risks in the areas of cybersecurity; 24) the development and implementation of business continuity and recovery plans, as well as information security management systems; 25) supervision over the cybersecurity risk estimation process; 26) the preparation of recommendations, standards and good practices in the area of cybersecurity, in particular enhancing the security level of information systems at the disposal of the entities of the national cybersecurity system; 27) the day-to-day maintenance and development of own relevant information systems; 28) the identification of hardware and software vulnerabilities in the supervised information and communication systems; 29) initial incident handling; 30) securing digital footprints; 31) the identification of cybersecurity threats; 32) the identification of operators of essential services and related procedures; 33) supervision over entities of the national cybersecurity system; 34) supervision of entities providing cybersecurity services; 35) conducting campaigns aimed at raising awareness in the area of cybersecurity, in particular the organisation of workshops and training; 36) conducting analyses on the functioning of the national cybersecurity system, including legal and organisational solutions, standards and certification in the area of cybersecurity, along with the preparation of draft normative acts; 37) conducting analyses in terms of the fulfilment

by entities from a specific sector or sub-sector of the conditions qualifying an entity as an operator of essential services; 38) conducting inspections of entities of the national cybersecurity system, including entities providing cybersecurity services; 39) domestic or international cooperation in the area of cybersecurity.

The remuneration (salary) paid in connection with the performance of cybersecurity tasks by a person having high qualifications may be increased by an ICT benefit. An allowance (in the case of employees) or a consideration in cash (in the case of officers and professional soldiers) – an ICT benefit – may be granted to persons performing tasks aimed at ensuring cybersecurity in entities specified in the legislation. The mere performance of such tasks does not entitle them to special treatment in terms of remuneration. In order to receive an ICT benefit, two conditions must be met jointly: 1) the performance of cybersecurity tasks; 2) employment or service in the relevant entities. The benefits are paid from the Cybersecurity Fund.

The remuneration (salary) paid in connection with the performance of cybersecurity tasks by a person having high qualifications may be increased by the amount of an ICT benefit. An allowance (in the case of employees) or a consideration in cash (in the case of officers and professional soldiers) – an ICT benefit, may be granted to persons performing tasks aimed at ensuring cybersecurity in entities expressly indicated in the legislation. The mere performance of such tasks does not entitle them to special treatment in terms of remuneration (salary calculation). In order to receive an additional benefit, two conditions must be met jointly: 1) performance of cybersecurity tasks; 2) employment or service in the relevant entities. The benefits are paid from the Cybersecurity Fund (Czuryk, 2022b: 106).

8 Cyberspace Defence Forces

Under Article 26 of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, No. 78, item 483, as amended), the Armed Forces of the Republic of Poland serve to protect the independence of the state and the indivisibility of its territory and to ensure the security and inviolability of its borders, remain neutral in political matters and are subject to civil and democratic control. Neutrality in political matters is understood as refraining from participation in political life and from supporting any political party or organisation (Banaszak, 2009: 152). As stipulated in Article 11 (2) of the Homeland Defence Act of 11 March 2002 (Journal of Laws of 2022, item 655, as amended), hereinafter the HDA, the Armed Forces of the Republic of Poland are a hierarchical, uniformed armed formation, which constitutes an organisationally separate part of the state defence system. Their task is also to ensure security in cyberspace. Hence, for this purpose, the Cyberspace Defence Forces have been established.

The Cyberspace Defence Forces are also included in the Armed Forces of the Republic of Poland as its specialised component, as stipulated in Article 15 (4) of the HDA. They

are responsible for the full range of activities in cyberspace, in particular for the proactive protection and defence of the elements and resources of cyberspace fundamental to the Polish Armed Forces.

The powers of the Commander of the Cyberspace Defence Forces are defined in Article 23 of the HDA, including the command over military and organisational units of the Cyberspace Defence Forces. The Commander of the Cyberspace Defence Forces reports to 1) the Minister of Defence until the appointment of the Commander-in-Chief of the Armed Forces; 2) the Commander-in-Chief of the Armed Forces upon his appointment and assumption of command of the Armed Forces. The powers of the Commander of the Cyberspace Defence Forces also include 1) the implementation of the development programme of the Armed Forces of the Republic of Poland; 2) designing, planning, organising, conducting and supervising training courses under the jurisdiction of the Commander of the Cyberspace Defence Forces for subordinate military and organisational units, as well as other institutions, authorities and entities based on concluded agreements; 3) planning and organising the mobilisation, development and use of the Cyberspace Defence Forces; 4) the construction, maintenance and protection of infrastructure, as well as the protection of data in cyberspace; 5) conducting activities and operations in cyberspace; 6) providing support for military operations conducted by the Armed Forces, and as part of alliances and coalitions; 7) cooperation with other bodies and entities in matters related to national defence; 8) managing and conducting inspections of subordinate military and organisational units. The Commander of the Cyberspace Defence Forces performs his tasks with the assistance of the Cyberspace Defence Forces Command.

The Cyberspace Defence Forces may also operate outside the country's borders. Military units of the Armed Forces of the Republic of Poland may be present outside the country's borders in order to participate in 1) an armed conflict or in order to strengthen the forces of the state or allied countries; 2) a peacekeeping mission; 3) missions to prevent acts of terrorism or their consequences; 4) the evacuation of citizens of the Republic of Poland, in the event of the need to protect their life or health, from a country that is not a member state of the European Union, a member state of the European Economic Area or a party to the North Atlantic Treaty – Article 2 (1) of the Act of 17 December 1998 on the principles of use or stay of the Armed Forces of the Republic of Poland outside the borders of the state (consolidated text, Journal of Laws 2021, item 396, as amended). The legislation refers to the presence of military units (Cyberspace Defence Forces) outside the state borders. What is meant here are organisational units of the Armed Forces of the Republic of Poland functioning based on the powers assigned to them by the Minister of National Defence, which use an official seal with the emblem of the Republic of Poland and the name (number) of the military unit (Article 2 (12) of the HDA).

It should be emphasised that, unlike other domains in which combat is associated only with open confrontation, combat in cyberspace is a permanent process, as well as a threat to potential targets or accidental victims (Marczyk, Pilarski, 2021: 311).

9 The Central Cybercrime Bureau

The Police Service was established as a uniformed and armed formation, the tasks of which are to serve the public, protect the safety of people and maintain public security and order. The aforementioned status of the Police is stipulated in Article 1 of the Police Act of 6April 1990 (consolidated text, Journal of Laws 2021, item 1882, as amended). What is required to effectively pursue this objective is not only the implementation by the Police of its basic tasks but also appropriate coordination of activities and close cooperation with state law protection institutions (Kotowski, 2012: 143-144). Security is also ensured by the Police by combating cybercrime. This task requires specific competence and knowledge, also in the field of new technologies, which are used to commit offences. Such crimes are dealt with by the Central Cybercrime Bureau (CCB).

As stipulated in Article 5d of the Police Act, the CCB is an organisational unit of the Police for combatting cybercrime, responsible for the implementation of tasks within the entire country in the sphere of 1) the recognition and combating of crimes committed with the use of an IT system, an ICT system or an ICT network, as well as the prevention of these crimes and prosecution of their perpetrators; 2) providing, to the necessary extent, support to organisational units of the Police in the identification, prevention and combating of cybercrimes, as well as prosecution of their perpetrators. The CCB Commander, who is in charge of the entire Bureau and its police officers, reports to the Police Commander in Chief. The seat of the CCB Commander is the capital city of Warsaw. The CCB Commander is appointed from among Police officers and dismissed by the minister competent for internal affairs at the request of the Police Commander in Chief. The deputies of the CCB Commander are appointed from among Police officers and dismissed by the Police Commander in Chief at the request of the CCB Commander. Should the position of the CCB Commander become vacant, the Police Commander in Chief entrusts the relevant duties to one of his deputies or a designated Police officer for a period not exceeding six months, until a new Commander is appointed. In order to perform statutory tasks, the CCB Commander cooperates with other organisational units of the Police and with competent authorities and institutions, including those of other countries.

The tasks of the CCB Commander are defined in Article 9 of Order No. 1 of the Police Commander in Chief of 12 January 2022 on the provisional organisational regulations of the Central Cybercrime Bureau (Journal of the National Police Headquarters of 2022, item 45), including in particular: 1) planning, organising and coordinating tasks to be performed by the CCB organisational units and exercising direct supervision over the activities thereof; 2) ensuring appropriate conditions for the proper performance of

official duties by subordinate police officers and employees; 3) exercising the powers and duties of a superior in relation to subordinate police officers and employees; 4) appointing police officers or employees to coordinate the work of the CCB teams; 5) participating in the development of draft material, renovation, and investment plans; 6) requesting changes to the schedule of works and expenditures of the CCB, in terms of purchases made, on the basis of separate regulations, by the Police Logistics Bureau and the Communications and IT Bureau of the National Police Headquarters; 7) managing the allocated resources within the scope of powers granted by the Police Chief Commander; 8) incurring expenditures within the scope of the allocated resources; 9) performing tasks arising from separate regulations related to the management of funds from the Police Operational Fund.

Under Article 11a (3) (2) of the Act of 21 June 1996 on Special Forms of Supervision by the Minister Competent for Internal Affairs (Journal of Laws of 2021, item 2073 as amended), the Internal Supervision Inspector may, based on information, including classified information, held by state services and entities subordinate to or supervised by the Prime Minister, the minister competent for internal affairs, the minister competent for public finance, the Minister of National Defence and the Minister of Justice, as well as data contained in registers, records and databases maintained by them, including classified information, subject candidates for the position of CCB Commander, Deputy CCB Commander, as well as persons currently occupying these positions, to verification.

The achievements of technological development often become tools used to commit crimes, while also being the target of criminal activity. Such crimes pose a serious challenge to the state authorities in terms of their identification, investigation and combating. Given the above, the legislator deemed it necessary to create a nationwide organisational unit of the police and establish a new service responsible for the identification, prevention and combating of cybercrime – the Central Cybercrime Bureau (Pawelec, 2022: 131). Cybercrime directly harms the security of cyberspace, and therefore special attention should be paid to ensuring protection against, and combating, such crimes, especially given the fact that the use of cyberspace is widespread, including for purposes such as implementing tasks of fundamental importance for the state and its security (Krupa: 2022: 164).

Chapter III

Cybersecurity in the Slovak Republic

1 Criminal law protection of security interests and cybersecurity

The Slovak Republic in the process of guaranteeing security, building the security strategy, building its security policy, and creating an adequate security system is based on the historical experience, available scientific analyzes and the forecasts of the security situation in the world, the Europe and on its own territory.

The attention of society has always focused on the two basic areas of security, namely the internal security and external security, and the corresponding sources of threats that have been basically presented by the natural and civilization sources of threats or the combinations of them. It is precisely the area of civilization threats associated with the armed violence that has become a region of great development in the mankind's historical development and has provided the humanity with the instruments of self-destruction, destruction of the world, and human civilization. The state uses the available tools of the security system to eliminate them, in the context of collective defense and safeguarding of protected interests, in the individual security sectors (Kelemen, 2014: 9).

The protection of state security by the standards of criminal law is one of the keys, legally protected interests. Today's empirical empowerment confirms that the security is a significant multidimensional factor of the quality of society and citizen's life, which we must systematically examine, forecast, and ensure.

The Slovak Republic is currently experiencing a new stage in the definition of security interests from its independence, which reflects the newly formed Security Strategy of the Slovak Republic under the authority of the Ministry of Foreign Affairs and the European Affairs of the Slovak Republic and their implementation in the parallel strategic documents such as the Defense Strategy of the Slovak Republic and the Military Strategy of the Slovak Republic, in the Ministry of Defense of the Slovak Republic.

We perceive the security strategy as the theory and practice of the functioning of the State – the Community of State, aimed at achieving the general and long-term security objectives. The previous approaches and opinions as well as the basic postulates of security and defense are contained in the Security Policy Documents, discussed, and

approved by the National Council of the Slovak Republic in September 2005 – the "Security Strategy of the Slovak Republic" and the "Defense Strategy of the Slovak Republic" (National Parliament, Security strategy, 2005: 1). The country Strategy Papers were in the process of updating to respond to changes in the security environment by all available means of the Slovak Republic, based on the "Strategic Defense Assessment" in 2011 and a broad professional and layout debate. A key pillar of our direction was the "Strategic Concept of Security and Defense of North Atlantic Treaty Organization Members" adopted by the Heads of State and Government in Lisbon in 2010 to replace the 1999 Strategic Alliance concept. "The strategic concept must offer freedom with regard to the foreseeable development, with sufficient precision to be useful to Allied officials responsible for implementing the policy" (Nečas, Kelemen, 2010: 44).

The security interests of the Slovak Republic are based on the principle of guaranteeing the security of the citizen in accordance with international legal standards and constitution, and the basic civil and democratic values. The Slovak Republic recognizes and protects the values of freedom, peace, democracy, the rule of law, law, and justice, pluralism, prosperity, solidarity, respect for human rights and freedoms (Security Strategy of the Slovak Republic 2021).

The Slovakia's security interests are based on the following values: 1) protection of democratic values, basic human rights and freedoms and principles of the rule of law and international law in the world; 2) effective state crisis management and a comprehensive approach to security; 3) resistance of the state and society to security threats; 4) citizens' trust in the democratic state and independent public institutions and cohesion companies; 5) security and stability in the Euro-Atlantic area and its neighborhood; 6) a functional and stable Euro-Atlantic security architecture with an emphasis on efficiency and the ability of NATO and the EU to act in their areas of competence; strategic cooperation between NATO and the EU based on their complementarity; 7) NATO's credible deterrent and collective defense, transatlantic strategic the United States' partnership, and military presence in Europe; 8) a united, prosperous, safe, open, and globally respected EU; 9) an effective United Nations ("UN") capable of responding to existing and new global challenges and threats; 10) effective Organization for Security and Cooperation in Europe (hereinafter referred to as "OSCE"), primarily in conflict prevention, mitigating their negative impacts and building trust and dialogue between states; 11) effective conventional arms control regimes in Europe and non-proliferation of weapons of mass destruction; 12) intelligence protection and support in the protection and enforcement of security interests of the state; 13) the readiness of the state and society to respond effectively and in a coordinated manner to hybrid threats, including misinformation; 14) ensuring a functional system of cyber, information and communication security; 15) protection of the state's critical infrastructure; 16) effective screening of foreign investments for reasons of security and public order a risk capital control; 17) protection of the

environment, public health, and cultural heritage; 18) energy, raw material, environmental and food security; 19) sustainable development and prosperity of the state and society, inclusive and sustainable economic growth, sustainability of public finances, budgetary responsibility and transparency, social stability and cohesion, competitive economy, even regional development; 20) high level of education, research, and technological development (Security Strategy of the Slovak Republic 2021).

2 Protection of classified information in Slovakia

The protection of persons, property and security interests by the substantive criminal law rules are among the key, legally protected interests. Today's social empiricism confirms us that the security is a significant multidimensional factor of the quality of society and citizen's life, which we must systematically examine, forecast, and secure by the legal and criminological means. We can contribute to the fulfilling one of the basic functions of the state, which is undoubtedly to ensure the security of the state and the security of the citizen.

One of the educational tools for examining the issue is also the study and scientific field of the Protection of People and Property, which is a related study and scientific field to the Law, Criminology, Criminalistics... and belongs to the science and technology departments of the legal science subgroup. The graduate is responsible for the management of institutional security structures, economic and business organizations and the systems used for the protection of persons and property, has knowledge of principles of technical means and legislation, is ready and able to effectively manage systems in the fight against the offenders who use state-of-the- in organized crime or terrorism. Providing the staff training in protection of persons and property is essential to protect the society (the state) from the negative anti-social phenomena, against various types of crime. In the field of concept, analytical activity, organization, control and security activities, graduates can analyze the security situation and propose optimal solutions aimed at the protection of persons and property, based on a scientific and creative approach. legally protected interests in the public and private sectors (Fields of study, 2022: 1).

The protection is the prevention of an adverse effect that can damage or destroy the protected subject (protected interest) by the applying preventive and/or repressive means (measures, standards). The protection processes are the starting platform for the complex security processes, the protection of security interests.

The protection of individuals means the active use of preventive and repressive instruments (measures, standards) for the protection of rights in relation to the physical status of persons defined and regulated under the public and private law. The legislation and protection of persons is thus ensured by the standards of several legal disciplines at the national and international level. Their starting points are the fundamental human

rights and human freedoms enshrined in the Second Chapter of the Constitution of the Slovak Republic and other laws (legal regulations) in our legal system, for everyday practical implementation and the specific legal circuits.

The property protection is, in the principle, the process of securing the security of a subject (protected interest) by the using of safeguards and standards aimed at the eliminating the security risk of an illegal activity or event that is contrary to the laws and the interests of the "possessor" of the protected interest. Regarding property, it should be noted that it may be tangible or intangible. The tangible assets include, for example, buildings, computing, transport, and so on. The intangible assets include, for example, software, licenses, patents, etc. Beyond the basic allocation of assets for the accounting purposes, we perceive the protected information and other legally protected security interests as the significant intangible assets. The protection of tangible property is realized within the so-called "physical and object security". The protection of intangible assets is, as a rule, implemented within the framework of several legal disciplines and legislation.

The physical and object security is a system of measures to protect an object (classified information, etc.) from the unauthorized persons and against the unauthorized manipulation in the objects and protected areas. The protection is provided by the mechanical barriers, technical security devices, physical protection, regime measures and their combination in accordance with the safety standards (set standards) of the physical security and object safety. The method, conditions and extent of the proposed measures are determined by their supervisors based on an assessment of the risks of possible threat to objects and protected areas (National Security Office, 2022: 1).

The information resulting from the physical and mental integrity of a person or systems (technologies, technologies) created by him and having the character of a protected interest (protection of classified information, protection of personal data, business secrets, espionage / industrial espionage and related unlawful activities,) are implemented mainly within the so-called " information security (with the emphasis on protecting classified information, in line with the state/EU cyber security concept). Cybernetics is a new operating domain, so we perceive the protected information as part of the security interests of the state. The National Authority in the Slovak Republic and the Central State Administration for the Protection of Classified Information, the Cipher Service, Cyber Security and Trusted Services (for electronic transactions in the internal market, electronic signatures, and stamps) is the National Security Authority, based in Bratislava.

The protection of classified information means the creating of conditions for the personnel security, administrative security, cryptographic information protection, physical security and object security, security of technical means, including the protection of foreign information. The obtaining a Certificate of Disclosure of Classified

Evidence of an Appellate Degree is not a basic prerequisite for the performance of their function but is accompanied by several obligations and procedures that lead to the security of classified information prior to their misuse (National Security Office, 2022: 1). The Office has a significant competence since 2016 for the cybernetic security, in coordination with the European Cyber Security Organization European Cyber Security Organization ESCO, based in Brussels.

For the purpose of the Act, the classified information is the information or matter designated by the originator of a classified information which, in view of the interest of the Slovak Republic, must be protected from being divulged, misused, damaged, improperly reproduced, destroyed, lost or stolen and which may arise only in the areas established by the Government of the Slovak Republic by its regulation (Act on the Protection of Classified Facts and on Amendments to Certain Acts 215/2004 effective from 01.01.2021. According to the law, the information may be the content of a document, drawing, drawing, photograph, graph, or other record, content of the oral expression, content of electrical, electromagnetic, electronic, or other physical transport medium. It can be a mass media with information, product, device, real estate.

The protection of persons and property, the primary safeguarding of protected information and other security interests is perceived in a wider and narrower sense as: 1) the protection of interests in the entire societal dimension, implemented and analyzed at the local, national, regional and the international level of security and the application of relevant standards of the criminal substantive law; 2) the exercise of the protection of interests in an individual dimension, implemented and analyzed at an individual level of security and the application of relevant standards of the substantive criminal law (to ensure the safety of a citizen, the protection of a particular private or corporate property, another law protected interest, etc.).

The protection of persons and property, primary the safeguarding of protected information and other security interests are carried out at home and abroad through: 1) the state security management by the building and developing the capabilities of defense, protection, and state rescue); 2) private security organizations; 3) institutions under the subordination of the Ministry of Internal Affairs and Justice, as well as the protection in the proceedings before the international legal institutions (by applying the legal norms).

The basis of the successful study of criminal law in relation to this issue is the already acquired knowledge of legal subjects whose teaching is preceded by the criminal law (Mašlanyová et al., 2016: 3).

The selected national sources of rights for the protection of persons, property, and other legitimate interests:1) Constitutional Act no. 460/1992 Coll. Constitution of the Slovak Republic, Second Chapter, Art. 12-54; 2) Constitutional Act no. 227/2002 Coll.

Constitutional Act on the State Security in Time of the War, War, Exceptional Condition and Emergency Status; 3) Act no. 387/2002 Coll. Act on the State Governance in Crisis Situations Out of Time of the War and War Condition; 4) Act no. 319/2002 Coll. Law on the Defense of the Slovak Republic; 5) Act no. 129/2002 Coll. on an integrated rescue system; 6) Act no. 473/2005 Coll. The Act on Providing Services in the Field of Private Security and on Amendments to the Certain Acts; 7) Act no. 215/2004 Coll. on the Protection of Classified Information and on Amendments to the Certain Acts as amended; 8) Act no. 154/2010 Coll. The European Arrest Warrant Act.

Selected international sources of the law: 1) Council Decision EU No. 2013/488 / EU on the security rules for the protection of EU classified information; 2) The Rome Statute of the International Criminal Court is the international treaty that founded the Court, 1998; 3) the NATO founding treaty, 4 April 1949; 4) Document C-M(2002)49 Security within the NATO; 4) the Hague Convention (1907), the four Geneva Conventions (GCs) (1949); 5) the Additional Protocol I (AP I), governing international armed conflict, and Additional Protocol II (AP II), governing non-international armed conflict.

3 Reflection of the act on cybersecurity in aviation education in Slovakia

Today's phenomenon is as hybrid threats to society, in the public and private spheres, in the national and international dimension. Not only information activities have dangerous potential, but also cyber threats and attacks on selected entities / critical infrastructure / state.

Cyber security has therefore become a priority for the international community.

In this area, the European Union set out in a joint communication to the European Parliament and the Council "Resilience, deterrence and defense: building strong cyber security for the EU". The document emphasizes the key idea that "Cyber security is essential for our prosperity and security" (Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building a Strong EU Cyber Security, 2017). "Our future security depends on transforming our ability to protect the EU from cyber threats: civilian infrastructure as well as military capabilities depend on secure digital systems. This was recognized by the European Council in June 2017 " as well as in the Global Strategy for Foreign and Security Policy of the European Union.

At the national level of the Slovak Republic, we find a reaction in the form of the legal norm of Act no. 69/2018, Coll. On Cyber Security and on Amendments to Certain Acts, with effect from 1 April 2018. Professional and legal aspects of legally protected

interests are therefore the subject of systematic and long-term examination (Kelemen, 2017: 11).

The main legislative basis of the new law was the Strategy for Information Security in the Slovak Republic (Government Resolution No. 270/2008), the Legislative Intent of the Information Security Act (Government Resolution No. 136/2010) and Government Resolution No. 328/2015 on the Concept of Cyber Security. The draft Act on Cyber Security and on Amendments to Certain Acts was prepared by the National Security Office of the Slovak Republic in cooperation with the Office of the Deputy Prime Minister for Investments and Informatization.

In its 2017 Joint Communication, the European Commission announced its intention to support the creation of a network of Cyber Security Competence Centers to stimulate the development and deployment of cyber security technologies. As a first step in this direction, the European Commission has mapped existing centers of expertise in cyber security (e.g., university department, research center, etc.).

The result of this mapping is the so-called "Cybersecurity Atlas" (index of existing EU cyber security centers). The aim of this Atlas is to become a valuable tool and reference for the cybersecurity community, which is looking for potential partners and pooling European resources.

According to the information provided by the Slovak Liaison Office for Research and Development in Brussels in addition, as early as 2018, the European Commission came up with a pilot project under Horizon 2020 to network national centers and create a new impetus in cyber security and technology development competences (Slovak Liaison, 2018: 2).

The solution to the problem at the national level is the identification of the "National Competence Center for Cyber Security of the Slovak Republic" at the National Security Office of the Slovak Republic, and possibly the creation of a consortium for its professional and legal support in implementing this agenda.

The resilience of networks and the stability of the information system is a prerequisite for the smooth and smooth functioning of the EU's internal market and a prerequisite for credible international cooperation. "Networks and information systems play a vital role in free movement and are often interconnected and interconnected by the Internet as a global tool. Disruption of the network and information systems in one Member State therefore affects other Member States and the EU as a whole, "explained the key issue of the new lawmaker, the National Security Office (Explanatory report, 2017: 1).

This problem cannot be comprehensively solved by one state, but by consistent and professional international cooperation based on high-quality national capabilities. The

Cyber Security Act transposed into Slovak law the European Directive on measures to ensure a high common level of security of networks and information systems in the Union (NIS). The NIS Directive is the first pan-European cybersecurity legislation aimed at strengthening the powers of national competent authorities, increasing their coordination between them, and providing security conditions for key sectors as a methodological guide for Member States.

The experience of the security community confirms that due to the mutual inconsistency of existing legal norms, in which the issue of cyber security was partially addressed in the Slovak Republic, the level of protection was diverse and incompatible, because of which it did not reach the required level of EU member states. The result is a failure to ensure an adequate level of cyber security against existing threats, resulting in irreparable losses, and undermining the credibility of organizations and the state.

"The goal of cyber security is therefore to minimize the possibility of such threats and, in the event of the consequences, to minimize their impact, which is a necessary condition for both public administration and the private sector" (Explanatory report, 2017: 8).

Already during the legislative process LP-2017-407, the comment procedure on the draft law, 706 comments were received, of which 236 were fundamental comments on the draft law. The analysis of the draft legal standard and the comments resulted in the following, selected fundamental outputs: 1) the proposal repeatedly referred to vague legal concepts which it does not define itself and which are not established in the current legislation. There was a requirement that the submitter of the law, in accordance with the valid Legislative Rules of the Government of the Slovak Republic, reduce the degree of uncertainty of these terms to prevent later problems of interpretation in the application of the law after its approval; 2) uncertainty of concepts brings other problems in application practice; 3) the wording of the draft law was objected to "For the purposes of ensuring the fulfillment of tasks under this Act, the Office may enter into a cooperation agreement with a natural person or a legal entity. The cooperation agreement must contain the specific form and conditions of cooperation. The cooperation agreement is not a compulsorily published agreement. "It completely violated any security measures of the basic service operator in personnel and physical security. According to the proposal, any person who has entered into an agreement with the Office will have the competence to consult any information. If the applicant maintains the possibility of concluding a cooperation agreement, it is necessary to set out the specific conditions that a natural or legal person as a contracting party must meet, including the provision of the obligation to demonstrate knowledge of security and technical standards, qualifications, and cyber security skills. The scope of the information with which such a person will be entitled to consult the basic service provider should also be laid down in a written agreement and the obligation to maintain confidentiality of the facts which that person has become aware of in the

implementation of such an agreement should be laid down. Also, if the agreement is not excluded from the mandatory publication of contracts under Act no. 211/2000 Coll. as amended, non-disclosure of this agreement is a violation of this law. Even in the case of unpublished contracts, however, there is an obligation to publish information on its conclusion (the so-called notification obligation); 4) the remaining problem in the case of new legal norms is to achieve compliance with other valid legal norms; 5) objected to the bill that "Members of the Office are authorized to enter the communication and information systems to the level of system administrator, including the right to temporarily change the hardware or software configuration, in connection with the performance of control and to the extent necessary for its performance". The proposed wording of § 29 par. 6 of the bill provides disproportionate competencies to members of the Office, including disproportionate interventions in communication and information systems. Pursuant to § 3 par. 4 of Act 275/2006 Coll. on public administration information systems, obligated persons who are IS administrators are obliged to ensure the smooth, secure, and reliable operation of public administration information systems under their administration, including organizational, professional, and technical support, and to secure the public administration information system against misuse. In the event of a change in hardware or software configuration, the provision of these obligations may be compromised or directly disrupted. At the same time, there may be a violation of the provisions of Act no. 122/2013 Coll. on the protection of personal data, as the right to enter the information system at the level of the system administrator may result in the disclosure of personal data of the data subjects, provided that personal data have been processed in the given information system. If the proposed wording of § 29 par. 6 of the Act on Cyber Security will not be repealed, the IS administrator cannot ensure the fulfillment of obligations imposed on him by Act no. The bill should also determine who will be responsible for the malfunction or disruption of IS functionality after a change in hardware or software configuration and who will bear the adverse consequences associated with it, including compensation for damage caused to third parties; 6) definition of cyber security incident in § 3 letter f) of the draft law largely overlaps with the facts of the criminal offenses specified in § 247-§ 247d of the Criminal Code. However, the bill in this provision, or elsewhere, does not address the interaction with criminal proceedings, does not refer to obligations in criminal proceedings and does not consider in several places, such as the need to secure evidence (response to a security incident should be conducted evidence for subsequent criminal proceedings). This is the complexity of the assessment of the proposed legislation (Comments raised, 2017: 1).

Legislative solution of selected outputs and problems: 1) for the purposes of ensuring the fulfillment of tasks pursuant to this Act, the Office may enter into a written agreement on cooperation with a natural person. The cooperation agreement must contain the specific form and conditions of cooperation and the natural person must be entitled to become acquainted with classified information of the appropriate classification level if the performance of tasks requires it; 2) in exercising control over

compliance with the provisions of this Act and its implementing regulations, the Office shall proceed in accordance with the basic rules of control activities established by a special regulation. For the purposes of the inspection, the basic service operator and the digital service provider have the rights and obligations of the inspected entity pursuant to a special regulation. The Office shall carry out an inspection at the digital service provider if there is a reasonable suspicion that the digital service provider does not meet the requirements set out in this Act; 3) cyber security incident means any event which, as a result of a breach of network and information system security, or a breach of a security policy or binding methodology, has a negative impact on cyber security or which results in loss of data confidentiality, destruction of data or breach of system integrity, restrict or deny the availability of a basic service or digital service, a high probability of compromising the activities of the basic service or the digital service; or threats to information security.

4 Cybersecurity in civil aviation in Slovakia

The basic document for solving the problem in civil aviation in Slovakia is the legal norm "Act on Civil Aviation (Aviation Act) and on Amendments to Certain Acts" (Act No. 143/1998 Coll.). This Act regulates the operation of aircraft in the airspace of the Slovak Republic according to the rules of flight applicable to civil aviation, in the field of civil aviation competence and authorization of members of aviation personnel, competence of aircraft and other aeronautical products, aircraft register, establishment and operation of airports and aircraft ground facilities , performance of air transport, aviation works and other business in civil aviation, protection of civil aviation, competence of state administration bodies and imposition of sanctions.

According to Section 2 of this Act, an act of unlawful interference means the communication of false information (in accordance with Section 180b of the Criminal Code) or the interruption of information flows necessary for the performance of air traffic, resp. reporting false information which may endanger the safety of passengers, flight crew, or ground staff at the airport, public order at the airport, or the smooth operation of air operations. The protection of cyberspace airports and air traffic is therefore important.

The issue of cybersecurity in civil aviation in Slovakia finds support in the legal norm, which is the Act on Cyber Security and on Amendments to Certain Acts, of 30 January 2018. The law was approved by the National Council of the Slovak Republic.

The Act transposed Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high level of security of networks and information systems in the Union into the conditions of Slovakia. It regulates the rights and obligations of persons as well as the authority and competence of public authorities by setting minimum requirements for the standard provision of important information

systems in the Slovak Republic. It lays down minimum requirements for ensuring cyber security in this Act and does not prevent the application of stricter security measures. The main goal is the protection and functionality of cyberspace.

In relation to civil aviation, within the organization of state administration bodies according to § 4 letter a) b) Ministry of Transport and Construction of the Slovak Republic. The Transport Office of the Slovak Republic performs this key role on behalf of the Ministry. Due to coordination, another important body of state administration in the field of aviation is the Ministry of Defense, which is responsible for the activities of the Air Force of the Armed Forces of the Slovak Republic. The cooperating state administration body is also the Ministry of the Interior of the Slovak Republic, which is responsible for the operation of the Squadron of the Ministry of the Interior (the so-called government squadron).

The state uses the Unified Cyber Security Information System, defined in § 8. The system serves for the management, coordination, registration, and control of the performance of the state administration in the field of cyber security and CSIRT units – Computer Security Incident Response Teams. The number of users connected to the Internet has grown dramatically in the last few years. However, their awareness in the field of information security is different, and this creates space for computer incidents, which may ultimately affect the very operation of the state. What's more, there is still a low probability that a potential attacker will be discovered. Given the above facts, it is important that the digital space of the Slovak Republic (resp. NIKI – National Information and Communication Infrastructure) is protected and potential incidents are resolved, their consequences mitigated or eliminated.

The main task of the specialized unit CSIRT.SK is to solve information and security incidents in the Slovak Republic in cooperation with owners and operators of affected parts of NIKI, telecommunications operators, Internet service providers and possibly other state authorities (e.g., police, investigators, courts). Furthermore, building and expanding public knowledge in selected areas of information security and cooperation with foreign sister organizations and the representation of the Slovak Republic in the field of information security at the international level (CSIRT.SK, 2022: 1). To coordinate national activities aimed at preventing and addressing ICT security issues, the international organization "FIRST" (Forum of Incident Response and Security Teams) was established in 1990, currently bringing together more than 180 CSIRT/CERT teams from around the world, of which members are: teams from government, commercial and academia. At European level, there is a TF-CSIRT group that facilitates the cooperation of CSIRT teams within Europe. The TF-CSIRT provides a space for the exchange of experience and knowledge in the field of information security, works on the development of common standards and procedures for responding to security incidents and helps in the creation of new CSIRT teams. Furthermore, the European Union Agency for Network and Information Security

ENISA was established in 2004, which ensures coordination and methodically assists in building new CSIRT teams or developing existing teams.

The unified information system of cyber security consists of a public and a non-public part – a public part with content according to § 8 par. 2 available on the portal of the National Security Office of the Slovak Republic, access to it is free of charge and takes place in real time. The law focuses primarily on the basic service, which means a service included in the list of basic services (including air transport) and depends on networks and information systems and is performed in at least one sector or sub-sector.

In the Transport sector, in the Air transport subsector, the basic services are: 1) air carriers – an air carrier with a valid operating license or equivalent; 2) airport managing bodies – an entity which, in connection with or without other activities, has, as the case may be, national laws, regulations or treaties to manage and control the airport infrastructure or airport network and to coordinate and control the activities of individual operators at the airports concerned; in the relevant airport networks, airports, including major airports, and entities operating ancillary facilities located at airports; 3) operators providing air traffic control (ATC) services as a service provided for purposes: a) collision avoidance, between aircraft, and – in the operating area between the aircraft and obstacles, b) accelerating and maintaining the proper flow of air traffic; 4) administrators and operators of networks and information systems, which are an element of critical infrastructure according to Act no. 45/2011 Coll. critical infrastructure or are directly connected to it. Basic service is an element of the state's critical infrastructure.

In connection with the Transport sector, we must also mention the Water and Atmosphere sector, where the Aeronautical Meteorological Service operates within the Meteorological Service, administrators and operators of the state hydrological network; administrators and operators of networks and information systems, which are an element of critical infrastructure according to Act no. 45/2011 Coll. on critical infrastructure or are directly connected to it; and administrators and operators of the state meteorological network.

The following impact criteria apply to the basic service: number of users using the basic service, dependence of other sectors of the basic service, the impact that cyber security incidents could have in terms of scale and duration on economic and social activities and state or national security interests, market share geographical distribution in terms of the area that could be affected by the cyber security incident, the importance of the basic service operator in terms of maintaining continuity of service.

The sector-specific criteria for the air transport sector, including airports and air carriers, rail transport and seaports, determine the specific criterion: the share of national transport and the number of passengers or freight operations per year. In accordance

with §17 par. 5 the service provider notifies the state authority that the criteria have been exceeded within 30 days of the finding.

A cyber incident in civil aviation networks is any event which, due to a breach of network and information system security or a breach of security policy or binding methodology, has a negative impact on cyber security or results in loss of data confidentiality, destruction of data or breach of system integrity, restriction or denial of the availability of the basic service or digital service, a high probability of compromising the activities of the basic service, or a threat to information security. Cyber security incidents are reported in accordance with Section 24 of the Act.

A cyber security incident is identified as a serious cyber security incident if it meets at least one identification criterion for the category of a serious cyber incident - specified in the draft decree. We recognize 3 categories of serious cyber security incidents: level I category; category II.; category III. For the identification criterion, the number of basic or digital service users affected by a cybersecurity incident is a limit of 15,000 for category I, 35,000 for category II, and 50,000 for category III. For the identification criterion, the duration of a cybersecurity incident according to the percentage of time specified in the service level rules, which belong to individual services, the limit is more than 40% of the time for category I, more than 60% of the time for category II., More than 75 % of time for category III. For the identification criterion of the geographical spread of a cybersecurity incident, the limit is at least a district for category I, at least a region for category II, the whole Slovak Republic for category III. For the identification criterion, the degree of disruption of the basic service or digital service, the limit is "partial" for category I, "complete" for category II, "complete without compensation" for category III.

For the identification criterion, the extent of the impact of a cybersecurity incident on the economic or social activities of the state is the limit of economic loss, the number of injured (dead), and the impact on public order.

An important agenda in ensuring cyber security in the field of civil aviation is the audit. The State Office (National Security Office of the Slovak Republic) may at any time carry out a cybersecurity audit of the basic service operator or request a conformity assessment body to carry out such an audit of the basic service operator to confirm the effectiveness of security measures taken and compliance with the requirements of this Act.

The personnel within the air transport ecosystem work in different workplaces, in different job positions. Individual human-caused failures, workflow incidents or technology failures in one section of airport information systems may jeopardize the integrity and security of the entire air traffic support system. For this reason, students are already preparing in three levels: general aviation education, training of aviation

specialists and training using virtual training and information, simulation, and communication technologies in the aviation environment. The proposed model makes it possible to divide students, future airport staff, into the following basic groups: security and safety, airline / airport management / operation, information technology (IT) and computers in aviation, and passenger management and services (air cargo and air passenger transport). For those interested in expanding knowledge and developing an academic and research discussion on civil aviation cyber security, we refer to our independent work on "Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport" (Kelemen et al., 2020: 1). There is currently no single method for developing risk management technologies by engaging expertise through an adaptive approach. An expert model for assessing airport NIS risks and incidents using fuzzy sets is an urgently needed task to improve civil aviation information security.

In the next period, the attention of the aviation community will be focused on the amendment to the Civil Aviation Act, which will also have an innovative impact on strengthening safety in civil aviation networks. Among other things, the legislator plans to establish a register of operators of unmanned aerial systems and unmanned aerial vehicles whose project proposal is subject to registration. In this agenda, Slovakia is only catching up with the other member states of the European Union. Flight safety is affected by the increase in drone activities near airports, both in controlled and uncontrolled airspace. The legal environment needs to strengthen tools against those who threaten air traffic safety and coordination, information security for the management, monitoring, transmission and sharing of data for the coordination of aircraft operations and unmanned aerial vehicles. In addition to civil air operations, the Act also applies, to a limited extent, to the operation of aircraft in military services, police services, customs services, or flights in the public interest in the airspace, with the appropriate designation or note in the flight plan. This agenda requires increased protection of information and some of it is subject to a special confidentiality regime from unauthorized persons.

The issue of cyber security of civil air traffic raises many praxeological issues at a time of dynamic technological development and human error, which must be addressed at the national and international level of cooperation and coordination.

5 Implementation of knowledge on cybersecurity in the transport sector, in aviation education

In addition to commercial successes, possible failures, modern air transport, its management and security also generate risks, such as potential danger to persons, property, and other legally protected interests. The current danger, in the form of security threats, manifests itself in the form of security incidents or other anti-social phenomena, which may also have a criminal law level. Huge amount of data within the

network operation of information systems and data repositories of civil aviation is an attraction and a potential target of cybercrime.

Cyber security in civil aviation operations is one of the important praxeological issues in examining the security and resilience of one of the elements of critical infrastructure. The topic has its limits and specifics at the national and European level. In an era of globalization, the free movement of people, goods, services, finance and information, its importance in international aviation, police and judicial cooperation is global. Cyberspace erases "natural boundaries and obstacles" to illegal activity on the road for political or ideological purposes, as well as material enrichment at the cost of violating the fundamental rights and freedoms of others or other legally protected interests in the public and private sectors. We have two introductory questions: what methodology and tool in the prevention of cybercrime we can use and what are the forensic purposes for surveillance in civil aviation network operations?

To process and examine most of the issue, we use an analytical-synthetic method based on critical thinking, shaped by the conceptual tools of "situational management of complex systems", situation management methodology (Madrasz, 2003: 73).

The method of situational management in the field of cyber security of civil aviation network operations, as a complex adaptive system, creates preconditions based on the application of information technologies and analytical activities, especially for: 1) the situational superiority of managers in decision-making compared to classical linear decision-making; 2) shortening the decision-making and management process in the management and operation of air traffic; 3) increasing the effectiveness of the intervention in the system in case of deviation from the standards, or in case of non-compliance with the required parameters; 3) providing up-to-date information (feedback) for the participants of the manager; 4) improving the quality of internal processes and the interoperability of components; 5) increasing the efficiency of the use of available human, financial, material, and technical resources, within the national system, in cooperation with organizations abroad.

Findings from the implementation of knowledge and the law on cyber security within the agenda of safety and security in aviation are reflected in the study programs for the training of new aviation professionals: 1) in the study program of the first level of higher education (Bc., 3 years) "Air Transport Management", for the specialization "Security in Air Transport", primarily in subjects such as: a) comprehensive airport protection, b) security legislation, c) safety equipment technology, d) airport security documentation; 2) in the study program of the second level of higher education (Ing., 2 years) "Air Transport Management", for the specialization "Safety and Security in Air Transport", primarily in subjects such as: a) security management, b) aviation operational safety, c) security legislation, d) air carrier security program, e) solving aviation emergencies, f) design of security systems in aviation; 3) in the study program

of the third degree (Ph.D., internal study 3 years, external study 4 years) "Air traffic management", primarily in subjects such as: a) air safety, b) information systems in air transport, c) airport security, d) air traffic control, e) sensors and electronics of security and safety systems.

The Slovak Republic in the process of guaranteeing security, creating a security strategy, creating its security policy, and creating an adequate security system is based on historical experience, available scientific analyzes and forecasts of the security situation in the world, Europe, Central Europe, and its own territory.

The company's attention has always been focused on two basic areas of security, namely internal security and external security, and the corresponding sources of threats, which in the basic understanding were presented mainly natural and civilized sources of threats or their combinations. It is precisely the area of civilizational threats associated with armed violence that has become, in the historical development of mankind, an area that has experienced grandiose growth and provided humanity with tools for self-destruction, destruction of the world and human civilization. The state uses available tools of the security system to eliminate them, in the context of collective defense and securing protected interests, in individual security sectors.

At the national level, we expect that the work of the "National Competence Center for Cyber Security of the Slovak Republic" will ensure the implementation of EU intentions in the field of strengthening cybersecurity, as well as the implementation of the provisions of the Act on Cyber Security of the Slovak Republic: 1) coordination and methodological guidance of activities from the level of national authority; 2) promoting the synergistic effect of the potential of relevant actors at national level (within and outside the Cyber Security Knowledge Alliance); 3) supporting research, technology innovation, production as well as cyber security education (at professional level, in civil society education, participation in the national curriculum at primary and secondary schools, implementation of prevention programs, university and other lifelong learning for critical sectors / subsectors) state infrastructure, etc.); 4) developing training capacities and capabilities for forensic crime investigation and cyber prevention and developing cyber-criminology for theory and practice in critical infrastructure sectors.

Non-standard behavior in the civil aviation network operation can take the form of unlawful conduct in a specific cyberspace, with criminal liability for damage to protected interests. In the field of aviation security, the professional community recognizes 4 segments of vulnerability: 1) air traffic management / civil aviation network operation; 2) aeronautical / on-board control systems; 3) airport / internal information network, passport control systems, etc.; 4) the Internet of Things.

The detection, monitoring and analysis of such non-standard behavior in civil aviation network operations in the context of security incident prevention can act as an effective

prevention tool in this cyberspace, for the following key purposes of forensic surveillance: 1) leakage of information; 2) network traffic tunneling; 3) anomalies indicating long-term port scanning and other attacker activities; 4) preparation for data theft and data theft; 5) unauthorized, automated data collection; 6) foreign equipment in the network; 7) violation of internal security rules.

To cope with these safety challenges even in aviation conditions, there is quality professional training in aviation education, which reflects the knowledge of science and real safety practice.

6 National Cyber Security Center SK-CERT

The current key body of knowledge is the "Report on cyber security in the Slovak Republic in 2021" (National Security Office, 2021: 88), which states that on January 7, 2021, by resolution No. 5/2021, the government approved the National Cyber Security Strategy for the years 2021 to 2025. It is a starting strategic document in the field of cyber security, which broadly determines the direction of the Slovak Republic in the field of cyber security for the next period. The strategy determines the basic principles of the cyber security management system in the Slovak Republic. They respect basic rights and freedoms in cyberspace, the legality, and mechanisms of the security system of the Slovak Republic, the complexity of the approach to the issue of cyber security, as well as the management of national cyber security through risk management. It also identified the most serious threats capable of disrupting the cyber security management system at the national level, endangering the functioning of the state and its citizens.

The strategy defines 7 strategic goals (priority areas): 1) a trustworthy state prepared for threats; 2) effective detection and clarification of computer crime; 3) a resilient private sector; 4) cyber security as a fundamental part of public administration; 5) strong partnerships; 6) educated experts and the public; 7) research and development in the field of cyber security.

The strategy also defines the main foreign policy partners, the method of implementation of the strategy and the method of its financing. For the practical implementation of the strategy, an action plan for its implementation is necessary, therefore the Action Plan for the Implementation of the National Strategy was created and approved by the government on July 14, 2021 of cyber security for the years 2021 to 2025.

The action plan contains 161 tasks, divided according to priority areas from the strategy. In total, 20 entities are involved in the action plan and are responsible for individual tasks. The National Security Office has established a permanent monitoring committee that will monitor and evaluate the implementation of the plan and the implementation of tasks. All interested entities are represented in this monitoring committee. The

monitoring committee met for the first time in December 2021 and will then meet regularly until 2025.

Representatives of the National Cyber Security Center SK-CERT actively participated in national and international activities and thus strengthened the position of SK-CERT and the National Security Office as a respected and valuable member of the security community. They participated in sac conferences, workshops, working groups and other formats, where they presented the state of cyber security in Slovakia, approaches to the protection of information assets, the legislative environment, and other related topics.

NCSC SK-CERT represented the office in expert organizations Trusted Introducer and FIRST. Even in 2021, NCSC SK-CERT was the only certified unit in the Trusted Introducer organization. However, we are seeing a positive trend in interest in Trusted Introducer membership, with 4 new security teams joining Trusted Introducer in 2021, demonstrating the growing need to expand the security community internationally.

National Security Office of the Slovak Republic and NCSC SK-CERT cooperated with all its partners and partner organizations in the field of cyber security, while this cooperation mainly consisted in sharing experience, exchanging operational information in dealing with cyber security incidents and best practice in protecting information assets. The most important activities were exchange of information and coordination in serious incidents with international scope.

NCSC SK-CERT has been issuing regular security bulletins and warnings as a regular preventive activity since the beginning of its existence. They contain warnings about vulnerabilities in systems and services. Security bulletins and alerts are distributed primarily to basic service providers and add-on service providers, but anyone can subscribe to these products free of charge.

The assessment of vulnerabilities included in bulletins and warnings follows the internationally recognized CVSS 3.1 methodology, which assesses software vulnerabilities and hardware products. Security bulletins are issued weekly and contain a set of medium and high severity vulnerabilities according to the CVSS 3.1 metric. Security warnings contain vulnerabilities of critical severity, but in the event of a major impact, NCSC SK-CERT also issues a warning about vulnerabilities of lower severity.

As the main contact point at the international level, the National Security Office cooperated with its foreign partners and partner organizations, through the EU Council's working platform Horizontal Working Group on Cyber Matters (HWPCI) and in the relevant external formats of the Commission, the Cooperation Group (NIS Cooperation Group), in the network of national CSIRT units, (CSIRT Network) and CyCLONe. Their main task is to ensure and intensify cooperation and share information between authorities responsible for cyber security of member states and their units.

Among the key priorities of the Cooperation Group is the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of networks and information systems in the European Union (Directive NIS) and the related application of individual tools. In 2021, other important topics such as "Joint Cyber Unit" were added to this task, ENISA presented a roadmap of needs for cyber security exercises and states shared their experiences regarding the most serious cyber security incidents and threats that they faced during of the year they hit (ransomware dominated).

During 2021, the EU CyberNet community of interested entities was established, which brings together national authorities and institutions operating in the field of cyber security, expert groups for the given field, think tanks and academic institutions based in EU member states. Membership brings many benefits, such as the sharing of mutual expertise, best practices, good practice, and lessons learned from previous cyber capacity building activities or ongoing external cyber activities. Office confirmed his interest in membership, later became a member, and in the next step his contact persons were nominated.

At the national level, processes of sharing and exchanging relevant information continued, as well as solutions to strategic and conceptual issues. Relevant entities (National Security Office, Slovak Information Service, Military Intelligence, Police Force, etc.) communicated and shared information on a regular basis, important for the security of the national cyber space, and participated in solving operational as well as strategic problems. They also participated in international exercises focused on cyber security and cyber defense.

At the national level, the National Security Office has covered a communication platform for operators of basic services, intended for sharing experiences and exchanging recommendations and commenting on essential legislative documents related to cyber security.

In 2021, the National Cyber Security Center SK-CERT made available its new tool for aggregating and analyzing information from open sources – TaranisNG. It is about the so-called open-source software that anyone can download and use for free. This software is mainly intended for security teams, security researchers and analysts, and today it has more than 280 downloads and is used in 4 EU countries and one non-EU country. The National Cyber Security Center SK-CERT also launched the pilot operation of the Unified Cyber Security Information System.

It is a multiple requirement of Act no. 69/2018 on cyber security, as well as of its implementation regulations, so that the providers of the basic service and the providers of the additional service perform their activities fundamentally regarding the identified

risks. And at the same time, that adequate security measures are always implemented based on a previous risk assessment.

Risk analysis determines the probability of a future harmful event, which may be caused by the abuse of an existing vulnerability of an asset, a potential threat in connection with existing security measures and the identification of impacts in the event of a violation of the confidentiality, integrity, or availability of the asset. However, the law does not propose a method that operators should use when analyzing risks.

For this reason, on December 13, 2021, the office published on its website the material Methodology for the analysis of cyber security risks for application in risk management processes in accordance with the requirements of Act no. 69/2018 on cyber security. The document is published as a standard in terms of the authorizing provisions of the law, therefore it is a binding regulation for obligated persons.

Although the methodology of risk analysis is the standard for Act no. 69/2018 on cyber security, the document is also applicable for the performance of risk analysis in the context of public administration information technologies, as the methodology is in full compliance with the requirements of Act no. 95/2019 on information technologies in public administration.

By publishing the risk analysis methodology, the office fulfilled one of the tasks of the Action Plan ahead of time implementation of the National Cyber Security Strategy for the years 2021 to 2025.

7 Activity of the Competence and Certification Center of Cyber Security in Slovakia

As an accredited conformity assessment body, CCCCS certifies cybersecurity auditors and managers and integrated management systems. In the context of cyber security, a combination of information security management systems according to ISO/IEC 27001:2013, together with IT service management systems according to ISO/IEC 20000-1:2018, business continuity management according to ISO 22301:2019 and quality management according to ISO 9001:2015. For all the management systems mentioned, as well as for assessing the professional competence of auditors and cyber security managers, the CCCCS has been granted accreditation decisions from the Slovak National Accreditation Service. As the only conformity assessment body in Slovakia, the CCCCS covers all assessment objects and valid certification schemes relevant to cyber security (National Security Office, 2021: 92).

CCCCS activities under the Cybersecurity Made in Europe brand are also a form of conformity assessment. Only qualified entities authorized by the European Cyber Security Organization (ECSO) are authorized to grant this trademark. CCCCS is also

one of the authorized partners that awards the mark in Europe. The brand builds awareness of the strategic value of companies and organizations in cyber security that develop business based on trusted European values. As an industrial marketing tool, it also enhances reputation with business partners, investors, and end users.

The CCCCS also conducts cyber security audits of operators of basic services to confirm the effectiveness of the security measures taken and to verify the fulfillment of the requirements established by law. This CCCCS capability is also supported by the office, when in accordance with § 29 par. 6, the office may at any time conduct a cybersecurity audit of the operator of the basic service or request a certified cyber security auditor to conduct such an audit of the operator of the basic service to confirm the effectiveness of the security measures adopted, and the fulfillment of the requirements established by this law. However, as a national industry and technology center, the CCCCS mainly acts as an expert organization, in two levels – consulting and expert.

Expertise is a specialized professional activity performed by experts, for the client, under the conditions established by law. Acts of expert activity are mainly expert opinion and its supplement, expert opinion or confirmation, expert statement, and explanation. Expert activity is carried out in accordance with Act No. 382/2004 Coll. on experts, interpreters, and translators, as amended.

CCCCS is registered in the List of Experts, Interpreters and Translators of the Ministry of Justice of the Slovak Republic under registration number 900293, as an expert organization operating in expert sectors: 1) 100200 – electronics; 2) 100400 – control technology, computer technology (hardware); 3) 100600 – electronic communications; 4) 100700 – estimation of the value of electrical equipment and electronics; 5) 100900 – computer programs (software); 6) 101000 – security and protection of information systems.

While forensics is a strictly formal forensic activity, CCCCS expertise in consulting activities is provided through a broad portfolio of consulting services. CCCCS offers more than 80 separate consulting services in various areas on its website. By adopting the regulation of the European Parliament and the Council of the EU no. 2021/887, the European Cybersecurity Industrial, Technology and Research Competence Center (European Cybersecurity Industrial, Technology and Research Competence Centre, abbreviated European Cybersecurity Competence Center – ECCC) and a network of national coordination centers were established in 2021. It was the duty of each member state to establish a national coordination center by the end of 2021, which will be part of the European network. The National Coordination Center (NCC) must be a public sector entity or a majority-owned entity of a Member State that performs public administration functions. CCCCS acts as NCC based on the decision of the National Security Office.

The tasks of the NCC through the CCCCS are mainly: 1) support of the cyber security community; 2) research support with the aim of facilitating and speeding up standardization and certification processes in accordance with the Regulation on Cybersecurity; 3) coordination of activities in cross-border projects; 4) identification and solution of professional cyber security challenges in individual industries; 5) providing financial support to third parties from grants awarded by the European Competence Center; 6) presentation of the results of the activities of the network, the community, and the European Competence Center at the state and regional level.

By the end of 2021, CCCCS has signed memoranda of cooperation with the absolute majority of relevant university workplaces that provide study programs and departments in the field of information asset protection, for example with the Technical University in Košice, the Faculty of Informatics and Information Technologies of the Slovak Technical University in Bratislava, and the Faculty of Security Engineering Žilina University, with the University of Pavel Jozef Šafárik in Košice, with the Faculty of Management of the Comenius University in Bratislava and with the Academy of the Police Force. An important role of the CCCCS is also the education of adults in information and cyber security, including security awareness campaigns.

Chapter IV

Cybersecurity in the Czech Republic

1 Cybersecurity in the Czech Republic – introductory issues

For the state, as a subject of international relations, the relevant threats include, in classical terms, internal and external factors. This is the most rudimentary division (Czaputowicz, 2008: 30-33) but, at the same time, it is debatable due to an increase in the links and relations in the international system of state and non-state actors and considering the cyberspace that is unlimited by physical borders. While omitting definitions of security itself (Stefanowicz, 1984: 18), (Zięba, 2008: 15-39), (Pawlikowska, 2004: 61-63), which is extensively researched in the literature, I will present some facts regarding a section, i.e. its one sphere: cybersecurity.

Cybersecurity threats have revolutionised approaches to security: they have forced its inclusion in national security strategies, shattered old paradigms regarding the methods of ensuring it and rules related to the regulation of international conflicts. Today, cybersecurity is one of the domains of any country's security (Karpiuk, 2021b: 234). The fact is that ensuring cyber-security for the state and the public administration that performs these tasks goes beyond cyberspace, and the consequences of cyber-attacks have consequences in the real world, and not virtual reality alone. The most recent cyberattacks carried out against public sector entities in the Czech Republic can be cited here as an example: 1) the Brno University Hospital in the Czech Republic suffered a cyberattack during the COVID-19 pandemic, forcing it to divert the patients and postpone surgeries. The incident was considered critical because the hospital is home to one of the largest laboratories in the Czech Republic conducting COVID-19 tests (Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak, 2020); 2) the Czech Capital Prague had been cyberattacks on their email systems. The mayor of Prague said it was a large attack, he added the damage caused was limited. (Czech Capital Prague, Labour Ministry Face Cyber Attacks, 2020); 3) the Czech railroads, regional airports, and a public administration portal have been facing cyberattacks from a pro-Russian hacker group Killnet (Russian Hackers Target Czech Websites in a Series of Cyberattacks, 2022).

An interesting solution that is used in the Czech Republic's cybersecurity strategy is a coherence between two key spheres of the government's activities, i.e. the security system and the policy of technological development. These two spheres of the functioning of any rational political entity make it possible to maintain an equilibrium

between security issues and the civilisational development of the state. Therefore, the Czech experience may prove helpful in developing such changes for strategies in strategic planning in the area of national security of other countries, not only those that form the Visegrad Group. This is a good way to combine defensive measures with modernisation, progress and the socio-economic development of the state. In addition, when building a cybersecurity strategy as an element of a broader state security strategy, one may not forget about the hybrid structure of ever-emerging new forms of activities in this sphere (Kaczmarek, 2022: 51). The Czech solutions in strategic planning in the field of cybersecurity demonstrate that, in the light of the high dynamics of changes taking place in the contemporary geopolitical situation and social reality, as well as the complexity of contemporary security, the consideration of this issue covers an increasing number of various areas. This requires an interdisciplinary approach to the defensive and offensive aspects not only of cybersecurity but security as such. The scope of security is thus broadening, with the result that dealing with it not only through the prism of threats and challenges but also risks and opportunities, makes dealing with it effectively an increasingly difficult and complex undertaking. This is reflected in the approach adopted by the Czech Republic in the construction of their cybersecurity system and the strategies being developed.

One should not forget about one specific issue. The challenge for the Czech state is to transfer the achievements of the private sector to the public sector and use this potential to create an effective e-government system. There is a stark contrast between the achievements of Czech companies in the field of digitalisation and the relatively slow progress of the ever-implemented e-Government project.

More importantly, much-needed systemic actions on nation-state structures may not be in isolation from cooperation on cybersecurity. These modern and complex international realities require increased regional involvement and cooperation (Gizicki, 2013: 11). And this is what the Czech Republic appears to be doing both by building its state cybersecurity system and by pursuing cooperation in the V4, EU or NATO area. However, is this cooperation evenly spread among the Visegrad countries as regards the states' involvement? In his monograph, M. Górka indicates that it is not; however, he emphatically posits that, despite their declarations of cooperation, the individual states perceive cyber threats differently, and thus their involvement in technological development differs (Górka, 2019).

2 Policy approach to cybersecurity in the Czech Republic

However, did the Czech political elite's interest in building a cybersecurity system come post factum? Definitely not. Although the first European law on cybersecurity was the Directive adopted in 2016 (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, 2016)

(referred to as the NIS Directive or NIS 1), interest in building a cybersecurity system in the Czech Republic was evident before that.[2]

The growing interest in cybersecurity in the Czech Republic is linked to the increasing reliance on the Internet and ICT. In the 1990s, each ministry or any other government body was self-sufficient or shared a local network: an intranet or LAN. These networks were isolated from the Internet and remote access was initially reserved for emergency situations only. Therefore, security measures focused on protecting intranet access points. The trend of the 1990s in the Czech Republic, however, was geared towards increasing the effectiveness of the public sector.

It is to be noted that in recent years, the Czech Republic has been excelling in the region in terms of the digitalisation of the economy and society, and the achievements of the private sector in this area place the country among the top countries in the European Union. Czechia ranks 19th of the 27 EU Member States in the 2022 edition of the Digital Economy and Society Index (DESI). The country's strongest performance is in the Human capital dimension. Czechia has made a relatively solid progress in the overall DESI score since 2017 which grew slightly more than expected by convergence curve, meaning that its score improved at a marginally higher pace than the score of the Union as a whole. Compared to 2021, Czechia's ranking improved in Digital public services and Connectivity but worsened in Integration of digital technology (Digital Economy and Society Index (DESI) 2022. Czechia, 2022: 3). The lack of ICT specialists is the biggest obstacle to digitalisation in the country.

In the economic sector, the Czech Republic is doing much better in cyberspace than the public sector: for example, Czech programmers are among the most talented in the world, as best evidenced by one of the world's most popular antivirus programs, which originated in the Czech Republic. Unfortunately, however, this positive picture of digitalisation is distorted by the country's large backlog in the development of public services and internet infrastructure (Wasiuta, 2021). In catching up with the commercial sector, the public sector is therefore trying to deal with the visible backlog, for example through the recent expansion of the catalogue of e-services in public administration (e.g. in 2022, the first-ever Czech census took place using an electronic format). In 2018, the Czech Government approved the cross-sectional strategic document Digital Czech Republic Resolution No. 629 of 3 October 2018 "Digital Czech Republic", which deals with all the effects of digitization on the economy and society. It is a set of concepts that create the conditions for the long-term prosperity of the Czech Republic. Its content can

[2] The Directive imposes a number of obligations on the Member States, obliging them, among other things, to establish specific institutions and to introduce mechanisms of cooperation. The Directive obliges all the Member States to guarantee a minimum level of national ICT security capabilities. Its provisions enable both a centralised system at the national level and the sharing of competences between different actors. However, the document provides for minimum harmonisation and, therefore, sets certain minimum conditions to be met. In doing so, it does not limit the ability of the Member States to regulate these issues more broadly and in a greater detail.

be defined as follows: "Strategy of Coordinated and Comprehensive Digitization of the Czech Republic 2018+". With regard to the digitalization of public administration and services, the Czech Republic lags significantly behind other states of the European Union. Out of the total Member States, the Czech Republic ranked 22nd in the category of digitalization of public administration in 2018 (Bokšová & Bokša, 2018: 13). There are also good signs of technological progress in administration: for the first time since 2007, a member of the Cabinet – Deputy Prime Minister – is directly responsible for digitalisation, particularly in the area of public services. So, one of the main obstacles to the process of digitisation of public services is the failure of public administration and regulations to adapt to the pace of new technologies.

Despite the technological differences and advances in digitalisation between the public and commercial sectors, cybersecurity in the Czech Republic became an important national security issue after the year 2001. It is true that potential threats related to the use of the Internet were evident before, but they were relatively small compared to other problems of a state or regional security nature (Rezek, 2012: 31). However, it may be stated that cybersecurity policy in the Czech Republic is characterised by relative sophistication compared to the digitisation of public administration and consistency in its development. Cybersecurity issues have also been an integral part of international cooperation for almost a decade. The Czech National Security Agency (Národní Bezpečnostní Úřad, NBU) has successfully been pursuing a policy of international cooperation in this area since 2011, including joint exercises and simulations, and has initiated inter-state contact groups. The National Cybersecurity Centre (Národní centrum kybernetické bezpečnosti, NCKB), established as part of the Agency in 2014, serves as a good example of an institution coordinating ICT security at the state level. The Czechs have been developing cooperation with NATO and EU states in the area of cybersecurity. In 2015, a new Memorandum of Understanding on Cybersecurity was signed between representatives of the Czech Republic and NATO. The Czech Republic was the first NATO member state to sign the document. The Memorandum constituted another step in the process of implementing an enhanced cyber defence policy (Enhanced NATO Policy on Cyber Defence). This was a continuation of the efforts undertaken by NBU since 2011, which coordinates cybersecurity issues at the state level. These efforts have resulted, among others, in the introduction of the Act of Cybersecurity into legislation: Zákon o kybernetické bezpečnosti (Act No. 181/2014 Coll. of 23 July 2014 on Cybersecurity and Amending Related Acts, as Amended, 2014), hereinafter referred to as a.c.s., regulating the rights and obligations of natural and legal persons as well as the competences and authority of the state administration in this area. This also included the establishment of the National Cybersecurity Centre (Národní centrum kybernetické ochrany, NCKB) in May 2014 together with a computer incident response centre (GOVCERT.CZ). In 2015, upon an initiative of NBU, a new Czech Cybersecurity Strategy for 2015-2020 was published followed by its update for 2021-2025. According to the vision presented there, the Czech Republic is not only aspiring to become a regional leader but it also wants to support collective defence in,

among other things, NATO structures (Gapiński, 2015). The North Atlantic Alliance appears several times in the strategy, including the context of adapting the cyber capabilities of the Czech armed forces to the NATO standards, as well as the need to strengthen international cooperation (apart from the NATO, this includes OSCE: the Organisation for Security and Co-operation in Europe and the International Telecommunication Union). The aforementioned cooperation constitutes one of the main objectives of the Czech policy, implemented through, among other things, the promotion of cybersecurity in the Central European region, the establishment of bilateral relations and participation in joint training exercises. One of the most important Czech projects has been the establishment of a platform for dialogue (the Central European Cybersecurity Platform, CECSP) including Central European countries. The initiative operates on the basis of a working contact group with the main objective being sharing experience, know-how and good practices in the area of cybersecurity. In terms of other activities, for example, in 2014, the Czech Republic, including France and the UK, joined the NATO Cyber Defence Centre of Excellence, CCDCOE. In addition, joint exercises for senior decision-makers were held in June 2015 upon an initiative of the Czech NBU and the European Defence Agency (EDA) to develop scenarios for strategies to respond to cyberattacks. The simulation involved 57 public and private sector representatives from the Czech Republic, Austria, Slovakia and Estonia, as well as representatives from the European Union and the CCDCOE.

In the years that followed, the focus was on a systemic approach to cybersecurity in the Czech Republic, in fact a three-sector (i.e. public, business and civic sectors) and two-directional (i.e. security and development planning) approaches. The following chronological outline of the documents and strategies presented demonstrates the determination on the part of Czech government in this coherent approach to cybersecurity: 1) White Paper on Defence (2011); 2) Act of Cybersecurity (2014); 3) Strategy of the Czech Republic in the field of cybernetic security for 2012–2015 (2012); 4) Action Plan for the National Cybersecurity Strategy of the Czech Republic for the Period from 2015 to 2020 (2015); 5) National Cybersecurity Strategy of the Czech Republic for the period from 2015 to 2020 (2014); 6) Concept of the Build-up of the Armed Forces of the Czech Republic 2025 (2015); 7) Long Term Perspective for Defence 2030 (2015); 8) National Cybersecurity Strategy of the Czech Republic for the period from 2021 to 2025 (2021); 9) Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025 (2021).

From a legal perspective, security measures in the Czech Republic were also influenced by two major laws in addition to others which were also related to cyberspace. The following acts need to be indicated here: 1) Personal Data Protection Act) (Act No. 101/2000 – Personal Data Protection Act, 2000); 2) Information Systems in Public Sector Act (No. 365/2000 – Public Sector Information Systems Act, 2000).

These two acts describe the most important legal grounds for the Czech Republic in terms of cybersecurity until these issues have been systematised in the form of a.c.s. If one were to look at the news in the sphere of cyberspace, the Czech Republic maintains a consistent policy of its presence in cyberspace. The Czech Republic was elected to the Council of the International Telecommunication Union (ITU), a UN agency whose standards influence the use of communication technologies worldwide (the Czech Republic Became a Member of the Council of the International Telecommunication Union, Which Decides on the Development of Communication Technology, 2022). This translates into an approach to the country's cybersecurity policy.

3 Cybersecurity strategy of the Czech Republic

After outlining the specific genesis of the Czech Republic's approach to the issue of cybersecurity, the security strategy will be discussed in the context of cybersecurity with reference to its two most recent updates: from 2015 and 2020.

The Czech Republic's National Cybersecurity Strategy and the associated Action Plan were drafted by the Czech National Security Authority and adopted by the Government in 2015. Both cover the years 2015 to 2020. The previous strategy covered the years 2012 to 2015.

The need to update the strategy was addressed by the Czech National Security Council in June 2014. The National Cybersecurity Strategy of the Czech Republic for the period from 2015 to 2020 is a government document, developed in cooperation with the Chancellery of the President, the Parliament and other governmental and non-governmental bodies. The document emphasises that one of the objectives of developing a security strategy is to establish broad-based cooperation among Czech political groupings, which allows it to be referred to as a cross-party security solution. It also points out that the Czech national security strategy documents are in line with the international obligations resulting from the Czech Republic's membership in the North Atlantic Treaty Organisation, the European Union, the United Nations and the Organisation for Security and Cooperation in Europe (Ministry of Foreign Affairs of the Czech Republic, 2015). The security strategy under discussion consists of an introduction and four substantive chapters entitled: Security Policy of the Czech Republic, Security Interests of the Czech Republic, Security Environment and Strategy for the Implementation of Security Interests of the Czech Republic. The layout of the document thus reflects the requirements of the classic procedure undertaken to develop a national security strategy. What is apparent in this procedure is an inclusion of a continuous strategic cycle, with a logical sequence of cause and effect and successive elements that make up an overall and coherent study. These elements include a review of national interests and strategic objectives in the area of national security, a diagnosis and forecast of the security environment, a review of the operational concept and an assessment of the national security system (Security Strategy of the Czech Republic

2015, 2015). In the case of the Czech security strategy, all these elements are included; in addition, the operational strategy and the preparation strategy are included in one chapter. Being described in this clear manner, the strategic cycle forms a message indicating the direction the Czech government will be pursuing in cybersecurity planning in the long term.

What is noteworthy is the fact of the 'foresight' and future-oriented approach in the planning strategy. This technique, among planning techniques and techniques for studying the environment as forecasting focused on methods to predict the future by means of modelling (Müller & Müller-Stewens, 2009: 20-21), allowed the Czech authors of the strategy to perceive as early as a few years ago the growing importance of non-military threats (i.e. growing competition for securing access to energy resources, ageing of European societies, uncontrolled migration, transmission of infectious diseases, attacks in cyberspace, interdependence of financial markets, misuse of information and communication technologies, growing social disparities related, for example, to the expansion of poverty areas, the economic and social backwardness of some regions, exclusion, etc.). What was highlighted was that some of the changes taking place in global economic markets may be associated with the weakening role of the United States and Europe in the world, with a consequent weakening of alliance ties and a reduction in defence capabilities within NATO. The projected weakening of the role of states as those actors on the international stage that possess forces, means and tools to effectively fulfil regulatory and control functions was highlighted. Particular attention was paid to the increasing role of non-state actors (Security Strategy of the Czech Republic 2015).

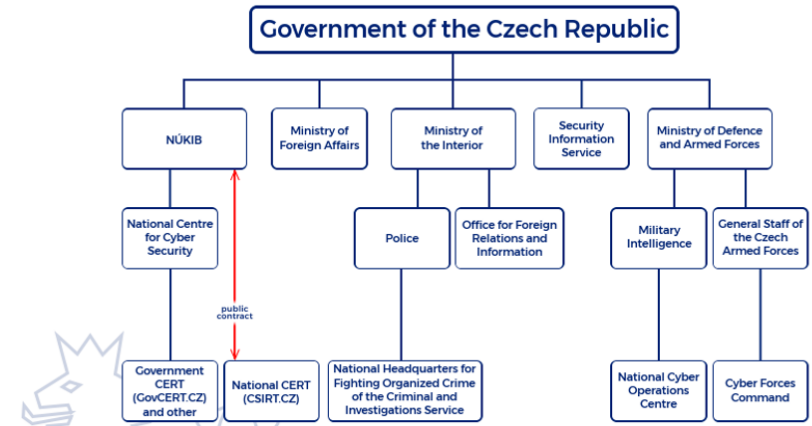
The consistency with which the Czech state takes a systemic approach to building state cybersecurity can also be seen in the next update of the strategy. In the Czech Republic, the basic act on cybersecurity is a.c.s., which implements the EU NIS Directive. It is consistent in its content and organisation with the guidelines of the latest version of the cybersecurity strategy. The Czech state's current cybersecurity strategy is contained in a document adopted by the government in November 2020 entitled "National Cybersecurity Strategy of the Czech Republic for 2021-2025" (Národní strategie kybernetické bezpečnosti České republiky na období let 2021–2025), which is an update of the previous cybersecurity strategy (Národní strategie kybernetické bezpečnosti České republiky na období let 2015–2020).

As indicated in the 2021 national cybersecurity strategy, the cybersecurity assurance system in the Czech Republic is based on a on a number of actors, with the government as the chief executive body playing the key role. As reported in the strategy, the Czech Republic's approach to cybersecurity is based on the cooperation of actors at the national and international levels, while it is particularly important to precisely define the scope of the competences and powers of individual institutions. It points to the rapidly evolving security situation, including the growing phenomenon of the risk of espionage

both against state institutions and private companies or scientific and research institutions. The strategy also highlights the growing importance of military operations in cyberspace. In this context, as indicated in the strategy, it is important not only to focus on current cybersecurity threats, but also to be able to adapt to new and ever-changing security conditions. The current strategy identifies cybersecurity objectives for the period up to 2025, which are divided into three areas: 1) cyberspace awareness (a common approach to cybersecurity, strengthening infrastructure security, effective communication strategy, information sharing, etc.); 2) strong and reliable alliances (effective international cooperation, promotion of the state's interests abroad, export of the so-called know-how, etc.); 3) Resilient Society 4.0 (secure e-government, education, building an expert base).

The strategy is complemented by the Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025 (Action Plan for the National Cybersecurity Strategy of the Czech Republic from 2021 to 2025, 2021). Achievement of the main goals of the National Cybersecurity Strategy of the Czech Republic is subject to the successful implementation and timely fulfilment of the tasks defined in this Action Plan for the National Cybersecurity Strategy. Certain tasks defined by the Action Plan require a close cooperation between the public authorities and other entities subject to a.c.s., as amended, and other public administration institutions. Each such task is to be coordinated by a designated body, which may require the cooperation of other entities. The designated bodies are responsible for fulfilling the tasks with the legal authority given and within their legally-defined range of competence. By the same measure, the roles and competence of individual institutions are not affected by this Action Plan.

Figure 1: Ensuring Cybersecurity in the Czech Republic based on National Cybersecurity Strategy of The Czech Republic 2021-2025



Source: National Cybersecurity Strategy of the Czech Republic 2020-2025: 8.

The Czech cybersecurity system is complemented directly and indirectly by other entities: central state administration bodies, offices, institutions or services, which will be mentioned here, but their role will not be discussed further here. For example, the Ministry of the Interior (Ministerstvo Vnitra České Republiky, www.mvcr.cz) has an influence on cybersecurity standards in the Czech Republic: it defines long-term goals related to the security of information systems and it promotes the issue of cybersecurity in the state as part of politics.

The Ministry of Defence (Ministerstvo Obrany České Republiky, www.army.cz) cooperates in the field of cybersecurity within NATO. The National Security Office (Národní bezpečnostní úřad, NBU, www.nbu.cz) is the central executive authority for the protection of classified information and security. It has been functioning since 1998 (Act No. 148/1998 Coll. on Protection of Classified Information and Amendments to Certain Acts of 1 August 1998., 1998). The Data Protection Authority (Úřad pro ochranu osobních údajů, ÚOOÚ, www.uoou.cz) is responsible for the protection of personal data regardless of the type of the system and, therefore, it has an influence on the cybersecurity standard as regards personal data.

Also, the Police (Policie České Republiky, PČR, www.policie.cz), in accordance with the criminal law, even in a case where there is a breach of cybersecurity, institutes legal proceedings. The Czech Police operates units that deal with cybercrime.

The Security Information Service (Bezpečnostní informační služba, www.bis.cz) is an intelligence agency active within the Czech Republic sine 1994. It is responsible for acquiring, collecting and evaluating information of major impact on the security of the country, protection of its constitutional setup and economic interests. It reports to the Government of the Czech Republic. The Service has the status of an armed security corps. Service officials are employed under a contract of service. They are entitled to hold and carry a service fire-arm and to use it for reasonable defense or in a situation of extreme distress – just as any other citizen (Who we are, 2022).

The Cyber Forces Command complements the Czech Republic's cybersecurity system as part of the military structure. In 2018, the Chief of the Headquarters of the Czech Armed Forces announced a plan to establish a cyber command. According to the Chief's declaration, the formation of this command was to take place in January 2019 and it was expected to achieve full operational capability only in 2025 (Czeska armia stawia na cyberbezpieczeństwo, 2018). Currently, in 2022, Cybernetic and Information Warfare forces provide the security and defense of Czech Republic in cybernetic and informational domains. They act either independently or within a domestic or allied framework, in close coordination with land, air and special forces. On tactical level, they monitor, plan and control operations in cybernetic and informational domain, including the support of STRATCOM of the Army of the Czech Republic. CIW forces provide the ability to defend domestic parts of cyberspace, conduct infoops, infoops in cyberspace, PsyOps and CMI/CIMIC. Within the cyberspace defense, they closely cooperate with Military Intelligence, and their individual capabilities complement eachother (Cyber Forces Command, 2020). The efficiency with which the Czech Republic moved from the declaration of objectives to implementation is another reason in favour of setting a policy for the development of a cybersecurity system.

4 Act on Cybersecurity of the Czech Republic

As already mentioned when discussing the current cybersecurity strategy, in the Czech Republic, the basic act on cybersecurity is a.c.s. (the text of the act in the Czech language is available at: https://www.zakonyprolidi.cz/cs/2014-181 and its amendments at: https://www.zakonyprolidi.cz/cs/2014-181/historie. Links to implementing acts or EU law: https://www.zakonyprolidi.cz/cs/2014-181/souvislosti). This fundamental act in the area of cybersecurity, including its complementary implementing provisions, implements the NIS Directive under EU law and it regulates the provision of the security of electronic communications networks and information systems. The Act is divided into five parts, and these are divided into individual paragraphs and clauses.

The first part of a.c.s. deals with cybersecurity, it regulates the rights and obligations of persons and the scope and powers of public authorities in the field of cybersecurity, yet it does not apply to information or communications systems handling classified information. The second paragraph defines the terms required to strictly define the sub-

elements of cybersecurity: 1) cyberspace: the digital environment that enables the creation, processing and exchange of information, consisting of information systems as well as electronic communications services and networks (taking into account the provisions of Act No. 127/2005 Coll. on Electronic Communications and on Amendments to Certain Related Acts (the Electronic Communications Act), as amended, 2005) hereinafter referred to: u.k.e.; 2) critical information infrastructure: an element or a system of critical infrastructure elements in the cybersecurity communications and information systems sectors (having regard to Art. 2 (Act No. 240/2000 Coll., on Crisis Management and on Amendments to Certain Acts (Crisis Act), as amended, 2000) and (Government Decree No. 432/2010 Coll. on Criteria for the Designation of Critical Infrastructure Elements, 2010); 3) information security: to ensure confidentiality, integrity and availability of information and data; 4) an important information system: an information system managed by a public body which is neither a critical information infrastructure nor a basic service information system, and where a breach of information security could impair or significantly impede the exercise of the powers of a public body; 5) an information system administrator: a body or a person that determines the purpose of information processing and the conditions for the operation of the information system; 6) a communication system administrator: a body or a person that defines the purpose of the communication system and the conditions under which it operates; 7) an information or communication system operator: a body or person ensuring the functionality of the technical and software resources that make up an information or communication system; 8) an important network, an electronic communications network: providing a direct connection abroad to public communications networks or providing a direct connection to critical information infrastructures (taking into account the provisions of the a.k.e.); 9) a basic service: a service that is dependent on electronic communications networks or information systems for its provision (within the meaning of Art. 2 Item (h) of a.c.s.) and a disruption which might have a significant impact on the security of social or economic activity in any of the sectors: energy, transport, banking, financial market infrastructure, healthcare, water management, digital infrastructure, chemical industry; 10) a basic service information system: a system the operation of which the provision of essential services depends on; 11) a basic service operator: a body or a person providing a basic service and designated by the National Cybersecurity and Information Office (Národní Úřad Pro Kybernetickou A Informační Bezpečnost – NÚKIB – In connection with their duties under Art. 22 a a.c.s.) for the purpose of fulfilling the information obligation (pursuant to Art. 5 Item 7 (Directive (EU) 2016/2102 of 26 October 2016 on the Accessibility of Public Sector Bodies' Websites and Mobile Applications (Text with EEA relevance), 2016). Authorities and persons providing "information security" and administering an "important information system" are also considered to be operators of basic services); 12) a digital service: an information society service in accordance with the Act regulating certain information society services (§ 2 a) (Act No. 480/2004 Coll., on Certain Information Society Services and Amendments to Certain Acts (Act on Certain Information Society Services), 2004), which involves the operation of the

following: a) an online marketplace that allows a consumer or a seller to enter into an online purchase contract or a service contract with a seller-entrepreneur, through the website of an online marketplace or the website of a seller who uses the service provided by the online marketplace, b) an Internet search engine that allows searches on any web page, based on a user's query about any topic in the form of a keyword, a phrase or any other input, with a service providing links where information related to the content requested can be found, c) cloud computing (hereafter referred to a.c.s.), which provides access to scalable and adaptable storage or computing resources that can be shared; 13) a competent authority: a body with competences in cybersecurity.

Bodies and persons with cybersecurity obligations in the Czech Republic include, according to Art. 2 of a.c.s: 1) a provider of electronic communications services and a provider of an electronic communications network; 2) a body or a person providing a core network; 3) the administrators and operators of: an information and communications system of a critical information infrastructure, a critical information system, the information system of a basic service; 4) an operator of a basic service; 5) a digital service provider. A supplementation of the obligations concerning the digital service provider is contained in Art. 3a: where a provider that provides this service in the Czech Republic is not established in the European Union and has not established a representative in another European Union Member State, they shall establish a representative in the Czech Republic. This is important because if a digital service provider is based outside the European Union and has established a representative in the Czech Republic, they are deemed to be based in the Czech Republic and subject to the obligations under a.c.s. However, where a digital service provider is based in the Czech Republic or has established a representative there, but the electronic communications networks and information systems they use are located in another Member State, the Czech Republic shall cooperate with the competent authority of the Member State concerned in the exercise of state administration.

Chapter two of a.c.s outlines security measures or rules for reporting cybersecurity incidents. The security measures as defined in Art. 4 a.c.s. mean a set of measures to ensure the security of information in information systems and the availability and reliability of electronic communications services and networks in cyberspace. Importantly, taking into account the requirements of the security policy, security rules, security measures and other conditions that are necessary to fulfil the obligations under this Act (primarily in Art. 4) shall not be considered to be an unlawful restriction of competition or an unjustified impediment to competition. Security measures are divided into organisational technical measures (Art. 5 a.c.s.). Organisational measures include: an information security management system; risk management; security policy; organisational security; establishment of security requirements for suppliers; asset management; human resources security; traffic and communication management; access control; acquisition, development, maintenance and cybersecurity occurrence or incident management. This also involves business continuity management; and control

and audit. Technical measures, on the other hand, were categorised as physical security. First of all, a number of specific tools for the purpose of cybersecurity provision were identified: tools to protect an integrity of communications networks; tools to verify user identity; tools to manage access authorisations; tools to protect against malicious codes, a tool to record the activities of an information or communication system, its users and administrators; tools to detect cybersecurity occurrences; tools to collect and evaluate cybersecurity incidents; security of applications; cryptographic resources; tools to ensure the level of availability of information; industrial systems and monitoring systems security.

The administrator of a critical infrastructure information system, an ICT system of a critical infrastructure or any relevant information system may, pursuant to Art. 6 a.c.s., commission the operation of a critical infrastructure information system, a critical infrastructure ICT system or any relevant information system to another body or person (unless this is excluded under another Act).

Art. 7 defines a "cybersecurity occurrence" (Kybernetickou bezpečnostní událostí) and a "cybersecurity incident" (Kybernetickým bezpečnostním incydentem). A cybersecurity occurrence is an occurrence that may cause a breach of information security in information systems or a breach of the security of services or the security and integrity of electronic communications networks. An incident will then be known as a breach of the security of information, services and of the integrity of the aforementioned systems as a result of a "cybersecurity occurrence".

The rules for reporting cybersecurity incidents are set out in detail in Art. 8 a.c.s.: 1) authorities and persons with cybersecurity responsibilities in Art. 3 a.c.s. (under Items b-f, i.e. an authority or person providing the core network – unless they are a controller or operator of a critical infrastructure communications system; an administrator and operator of a critical information infrastructure information system, an administrator and operator of a critical information infrastructure communications system, an administrator and operator of a critical information system, an administrator and operator of a basic service information system – unless they are the administrators or operators of an information system or a critical information infrastructure information communications system) are required to report cybersecurity incidents in their critical networks, critical infrastructure information systems, critical infrastructure ICT systems, basic service information systems or critical service information systems to the basic service operator immediately upon detection; 2) without undue delay, the digital service provider shall report a cybersecurity incident that has a significant impact on the provision of their services, provided that they have access to the information necessary to assess the significance of the impact; 3) in general, a body or person providing the core network as well as an administrator and an operator of a critical information infrastructure information system report cybersecurity incidents to the national CERT operator. The CERT ensures an exchange of cybersecurity information at national and

international levels and acts as the Computer Security Incident Response Team. The function of the national CERT of the Czech Republic is performed by the CSIRT.CZ Team (About Team, 2022). More information on both public administration entities: NÚKIB and CERT operating in the area of cybersecurity is presented in separate subsections of the present paper; 4) in turn, cybersecurity incidents are reported to the National Cyber and Information Security (Národní úřad pro kybernetickou a informační bezpečnost, hereinafter: NÚKIB), which acts as the national single contact point for network and information systems security (according to Art. 22 a.c.s.). These are reported by the administrator and the operator of a critical information infrastructure information system, the administrator and the operator of a critical information infrastructure communication system, the administrator and the operator of a critical information system, the administrator and the provider of a basic service information system, and the provider of a basic service.

Incidents that have a significant impact on the continuity of services shall be reported by key services operators (provided that they have access to the information required to assess the significance of the impact) immediately to NÚKIB. Other authorities and persons (not listed in Para. 3 Art. 8 a.c.s.) may report cybersecurity incidents to the national CERT operator or to NÚKIB. The implementing rules, in turn, define the types, categories and assessments of the significance of the consequences of a cybersecurity incident, as well as the details and the method to report the incident.

A cyber emergency state is defined in Art. 21 a.c.s. This means a state where the security of information in information systems, or the security of electronic communications services or the security and integrity of electronic communications networks is endangered on a large scale, and the interests of the Czech Republic within the meaning of the Act governing the protection of classified information could be compromised or endangered (Item 1 of Art. 21 a.c.s.). Another provision contained in the same Article of the Act states that the decision to declare a state of cyber emergency is made by the Director of NÚKIB. The information on the declaration of a state of cyber emergency shall be announced in a nationwide radio and television broadcast, with the operator of the nationwide television or radio broadcast being obliged to immediately publish the information on the declaration of a cyber emergency, without changing its content or meaning, without any compensation of the costs, when requested by NÚKIB. The decision to declare a state of cyber emergency shall take effect on the date as specified therein. A state of cyber emergency shall be declared for a period of time strictly necessary, however not longer than 7 days. This period may be extended by the Director of the Office; the total duration of the cyber emergency declared shall not exceed 30 days. During a cyber emergency declared, the Director of the Office shall inform the Government about the progress in relation to the cyber emergency and the current status of the threats that led to the declaration of the cyber emergency state. In a state of cyber emergency and in a state of emergency (as formulated in the Constitutional Act No. 110/1998 Coll., on the Security of the Czech

Republic, as Amended by Constitutional Act No. 300/2000 Coll., 1998), in the cases referred to in Art. 6 of the Act, NÚKIB is also authorised to issue a decision or measure of a general nature on the grounds of Art. 13 a.c.s. If, under a state of cyber emergency, it is not possible to resolve a threat to information security in information systems, or the security of services or the security and integrity of electronic communications networks, the Director of the Office shall immediately request the Government to declare a state of emergency.

National Cyber and Information Security Agency (NÚKIB) is the central administrative body for cybersecurity, including the protection of classified information in information and communication systems and cryptographic protection. It is also responsible for the implementation of the public regulated service of the global navigation satellite system under the Galileo programme. It was established on August 1, 2017 on the basis of Act No. 205/2017 Coll., Amending Act No. 181/2014 Coll., on cybersecurity and on amendments to related acts (above all, the Cybersecurity Act) (About NÚKIB, 2020).

In the fourth chapter of a.c.s., entitled: "Operation of the State Administration", Art. 21a provides for the establishment of NÚKIB (referred to in the Act as "the Office"), based in Brno, as the central administrative body responsible for the area of cybersecurity and for the selected areas of the protection of classified information, in accordance with the Law on the Protection of Classified Information and Verification Processes. Its revenues and expenditures constitute a separate chapter of the state budget. It is headed by a Director who is appointed by the Government after consultations in the Committee of the Chamber of Deputies responsible for security matters, and who is also dismissed by the Government. The Director of NÚKIB reports to the Prime Minister or a designated member of the Government.

The duties are detailed in Art. 22 a.c.s: 1) establishment of security measures; 2) emission measures; 3) exercise of state administration in the area of the security of information and communication systems that handle classified information and in the area of cryptographic protection; responsibility for the operation of the National Communications Security Centre, the National Centre for the Distribution of Cryptographic Materials, the National Centre for Compromised Radiation Measurements and the National Centre for Information Systems Security, which forms a part of it; also, it performs other responsibilities in accordance with the obligations arising from the membership of the Czech Republic in the European Union, the North Atlantic Treaty Organisation and international agreements which the Czech Republic is bound by, in selected areas of classified information protection; 4) maintenance of records in accordance with this Act and the law on classified information protection; 5) administrative penalties for non-compliance with the obligations set out in this Act and the Law on the Protection of Classified Information and Verification Processes; 6) duties of a coordinating body in a cyber emergency situation; 7) cooperation with entities and individuals that operate in the area of cybersecurity and cyber defence and,

in particular, with public corporations, research and development institutes and other CERTs, as well as with entities and individuals that operate in selected areas of classified information protection; 8) ensuring international cooperation in the area of cybersecurity and in selected areas of classified information protection; 9) negotiations and conclusion of international cooperation agreements in the field of cybersecurity and in selected areas of classified information protection, provision of preventive measures, education and methodological support in the field of cybersecurity and in selected areas of classified information protection; 10) research and development in the field of cybersecurity and in selected areas of classified information protection; 11) conclusion of a public agreement with the operator of the national CERT; 12) submission to the Ministry of Interior, in accordance with the Crisis Act, a proposal concerning the elements of critical infrastructure in the sector of communications and information systems in the field of cybersecurity operated by a state organisational unit; 13) identification, in accordance with the Anti-Crisis Act, of critical infrastructure elements in the sector of communications and information systems in the field of cybersecurity, insofar as these are not the elements referred to in Item m); 14) verification, every two years, as to whether the designation of the critical infrastructure elements referred to is up to date; 15) designation of a basic service operator and a basic service information system; 16) development and submission to the government for approval of a national cybersecurity strategy and an action plan for its implementation, and updates of the strategy at least every 5 years; 17) duties of a single point of contact for cross-border cooperation on cybersecurity in the European Union; 18) acting as the competent authority in the Czech Republic and the fulfilment of their notification requirements towards the European Commission and the Cooperation Group in accordance with the relevant European Union legislation; 19) disclosure of information to the public in relation to a cybersecurity incident in accordance with Section 12(3); 20) analyses and monitoring of cyber threats and risks; 21) exercise of competencies in relation to the public regulated service of an access to the European Galileo satellite navigation programme; 22) publication of the Office Journal on the Office's website; 23) other cybersecurity tasks as provided for in this Act and in selected areas of classified information protection in accordance with the Law on the Protection of Classified Information and Verification Processes; 24) performing the duties of a cybersecurity certification authority in accordance with Art. 58 of the Cybersecurity Act.

Another competence of NÚKIB is that it designates, by way of a decision, the operator of a basic service and the information system of the basic service provided that the sectoral and impact criteria are met. At least once every 2 years from the date of the decision, the said office shall verify whether the conditions for the designation of the operator of the basic service and the information system of the basic service are met. The Authority's decision on the designation of thane operator of a basic service and a basic service information system is not subject to appeal. The broad scope of the competences is evident, for example, in Art. 22 Item c of the a.c.s: NÚKIB and the operator of the national CERT, when processing personal data covered by Regulation

(EU) 2016/679 of the European Parliament and of the Council, does not have to restrict the processing of personal data if the data subject disputes its accuracy or objects to such processing; and may, in the exercise of its powers, use personal data for purposes other than those which it was collected for.

In addition, NÚKIB maintains a "log of cybersecurity incidents" (with reference to Art.9 a.c.s., which contains a detailed scope of the data stored in the log), and the data collected therein is made available to public administration bodies and other entities (the principles of data sharing are set out in § 9 of the Act) for the purpose of exercising their competences. The data may also be provided by NÚKIB to the operator of the national CERT, authorities exercising competences in the field of cybersecurity abroad and other persons operating in the field of cybersecurity to the extent necessary to ensure the protection of cyberspace (Item 4 Art. 9 a.c.s.). In addition, the Act ensures the confidentiality of whistleblowers: information, the disclosure of which could jeopardise the provision of cybersecurity or the effectiveness of a measure issued under a.c.s., or information stored in the incident log, on the basis of which it would be possible to identify the authority or person who reported a cybersecurity incident, shall not be disclosed under the provisions governing free access to information. The other record maintained by NÚKIB and indicated in the Act is the contact data register (Item 4 of Art. 16 a.c.s.) containing the contact details of incident reporters (their scope is indicated in Item 1 of Art. 16 a.c.s.)[3]. As actions required to protect information systems or services and electronic communications networks from a cybersecurity threat or cybersecurity incident or to address a cybersecurity incident that has already occurred, Art. 11 a.c.s. indicates: a "warning", "reactive measures" and "protective measures". NÚKIB issues a "warning" in relation to a cybersecurity threat by publishing it on its website and by notifying authorities and persons listed in its contact records. In addition, considering the protection of internal order and security, the protection of the life and health of people or the protection of the state's economy, it has the power to inform the public of the incident (or to request the authority or the person affected by the incident to do so on their own). NÚKIB may issue a decision where it imposes "reactive measures" to address a cybersecurity incident or to secure information systems or electronic communications networks and services, which constitutes the initial action. If the decision may not be served to the addressee in person within 3 days from the date of it being issued, it shall be delivered by being posted on the official board of NÚKIB, and it shall become enforceable at that moment. The Office may also issue a decision under the Code of Administrative Procedure and an appeal against the decision is with

[3] Contact details, according to a.c.s., include: a) in the case of a legal entity: its name or surname, its registered office address, its personal identification number or a similar number assigned abroad; b) in the case of a sole proprietor: their name or surname with a distinctive addition or further designation, the registered office address and the personal identification number; c) in the case of a public body: its name, the address of its registered office, the personal identification number, if one has been assigned, and the identifier of the public body, if no personal identification number is assigned, and the details of the natural person who is authorised to act for the body or the person referred to in Para. 3 u.c.s.c., in matters regulated by the said Act, i.e. the name, surname, telephone number and the e-mail address.

no suspensory effect (Items 1-2 of Art.13 a.c.s.). According to Art.14 a.c.s., as a "protective measure", NÚKIB issues the so-called "measure of a general nature", where the authorities and persons indicated in the Act specify the manner to increase the protection of the systems, services or networks administered, including a time limit for its implementation.

NÚKIB shall also exercise control in the field of cybersecurity. It determines how the authorities and persons concerned fulfil the obligations set out in this Act as well as in the decisions and measures of a general nature issued by NÚKIB, and how they comply with implementing regulations in the field of cybersecurity. In exercising control in the area of cybersecurity, in relation to offences involving non-compliance with the obligations imposed by the provisions of a.c.s., it may impose fines ranging from CZK 10,000 to CZK 5,000,000 (and, for individuals, up to CZK 50,000). NÚKIB therefore also conducts misdemeanour proceedings.

However, the operations of NÚKIB are also subject to control (pursuant to Art. 24a a.c.s.). This is the competence of the Chamber of Deputies, which appoints a special audit body for this purpose. The Auditing Authority consists of at least 7 members. The Chamber of Deputies determines the number of members in such a way as to ensure the representation of each parliamentary faction formed according to a political party or a political movement which the deputies stood for election for; the number of the members is always odd. It is only a member of the Chamber of Deputies that may become a member of the auditing body.

The National Cybersecurity Centre (Národní centrum kybernetické bezpečnosti, NCKB) is the executive section of the National Cyber and Information Security and Agency (NÚKIB). The National Cybersecurity Centre oversees ("The National Cybersecurity Centre" 2020): 1) The activities of the Government CERT Czech Republic (GovCERT.CZ); 2) Prevention of cybernetic threats to critical infrastructure elements, basic service information systems, important information systems, and selected public administration information systems; 3) Resolution of and coordination of resolutions to cybersecurity incidents at critical infrastructure entities, operators of basic services, and public administration bodies; 4) Awareness and educational activities concerning cybersecurity; 5) Cooperation with national and international organizations that participate in securing cyberspace; 6) Organizing and participating in cybersecurity exercises at the national and international level; 7) Cybersecurity research and development; 8) Representing the Czech Republic in cooperation with the Director's Office at international organizations active in cybersecurity; 9) Evaluating cybersecurity risks and taking the appropriate corrective and preventive measures; 10) Fulfilling international obligations and cooperating at the international level in implementing regulations stemming from Czech membership in NATO, the EU, and other international organizations within its jurisdiction as part of the Agency's security

policy; 11) Defining the Agency's cybersecurity communication strategy in cooperation with other organizational units at the Agency.

The cybersecurity system is complemented by its cooperation: service provision to commercial and civil sector actors. The National Cybersecurity Centre (NCKB) and its GovCERT.CZ team offer the following services that could help your organisation assure cybersecurity (Provided Services, 2022): 1) Coordination and Aid in Resolving Incidents. Resolving security incidents is among the government team's main activities. When reporting such an event, the team's experts are prepared to technically aid your specialists and provide advice for further preventive measures. If it's discovered that an incident targeted multiple entities, the team is prepared to coordinate a common approach to its resolution. The GovCERT.CZ team provides network data and log analyses as part of resolving an incident with the goal of identifying the method and effects of the incident. It also offers consultations to obligated entities whether there was an incident and not just an event by analysing the corresponding data. In light of the extensive cooperation established across various institutions, contacts can be provided for Czech security teams as well as foreign partners to resolve incidents that cross borders; 2) Detection System Project. As part of the created and expanded detection system, GovCERT.CZ processes cybersecurity events and metadata from network operation in the form of flow records from the perimeter of connected organizations. The goal of the project is to detect global problems that have multiple targets among organizations that must participate in the project. Blacklists and signatures that are published are then feedback for the participating partners. Finally, it provides early warnings about attacks that we detect at other organizations that could affect you as well; 3) Implementing Honeypots; 4) Penetration Testing; 5) Internal and External Tests; 6) Constant Vulnerability Scanning; 7) Vulnerable Service Detection; 8) Other Specialized Tests; 9) A Forensic Laboratory; 10) Securing Data; 11) Analysis Procedures and Results; 12) The Cybersecurity of Operational Technologies; 13) Educational and Research Activities; 14) OT Cybersecurity Course

This one-day course in industrial cybersecurity is meant for non-IT employees so they understand cybersecurity threats in industrial technologies; increase their awareness about current cybersecurity problems; the differences between IT/OT environments; general cybersecurity fundamentals; and the specifics of cybersecurity in industry. The course is concluded with a demonstration of a cybersecurity attack on industrial network elements. Network Forensic Analysis Course; Network Security Course.

Every country that connects its critical systems to the internet must be able to effectively mitigate security threats, react to incidents, coordinate their resolution, and effectively prevent incidents. The Computer Emergency Response Team (CERT)[4]

[4] CERTs, or Computer Emergency Response Teams, or Computer Emergency Readiness Teams, are those entities whose main objective is 24/7 Internet traffic monitoring and that take immediate action in the event of threats. For computer incident response teams, the terms: CERT or CSIRT are commonly used. The use of

ensures an exchange of cybersecurity information at national and international levels and it acts as the Computer Security Incident Response Team. A division or distinction between government and national CERTs is often encountered in countries' cybersecurity systems. There is no commonly accepted and formal definition of a governmental or national CSIRT; hence, usually when formulating their security strategies, governments use informal definitions provided by the European Network And Information Security Agency (ENISA) (Deployment of Baseline Capabilities of National/Governmental CERTs, 2012) confirming that different countries adopt different definitions of these concepts. Under these guidelines, the governmental CSIRT is responsible for the protection of government/public and state networks. Its "constituency" (Deployment of Baseline Capabilities of National/Governmental CERTs, 2012):8 includes the government and other public institutions. In the case of a national CSIRT, ENISA identifies a team to act as a contact point for sharing information with other national CSIRTs. The roles of the two teams: governmental and national ones may or may not be combined. Indeed, both ENISA and the Carnegie Mellon University CERT, which actively supports national CSIRTs, allow for the existence of multiple teams of this type within one country, without indicating the primacy of one over the others.

The function of the national CERT of the Czech Republic is performed by the CSIRT.CZ Team (About Team) and the Governmental CERT: GovCERT.CZ. Teams like the CERT play a key role protecting critical information infrastructure and important information systems according to the Law on Cybersecurity (181/2014 Sb.) and its implementation regulations. These teams also act as a source of security information and help state bodies, organizations, and citizens. They also play a key role in internet security education. Bodies and individuals subject to the Law on Cybersecurity must fulfil certain obligations to the Government CERT team and according to section 3 paragraph a) and b), bodies and individuals fulfil obligations specifically to the national CERT team. The CZ.NIC organization operates under the auspices of the national CERT team (Government CERT, 2022). There exists government cooperation with the private sector such as non-governmental CSIRTs, universities, banks and other entities has been taking place on an informal basis, and relations are mostly positive thanks to a long-term building of mutual trust. The Act of Cybersecurity brought since 2015 some formal obligations for the private sector. For example, ISPs have a duty to report incidents to the National CERT (as opposed to Government CERT), and in case of cyber emergency, they have to implement the measures prescribed to them by the NSA. Private sector operators of CII have yet more obligation CERT as a response team thus appears in the Czech cybersecurity system as: 1) The Governmental CERT (as part of NÚKIB); 2) The operator of the national CERT.

---

the term of "CERT" in the name of another team is only formally possible upon an approval of the Carnegie Mellon University. For this reason, the abbreviation of CSIRT (the Computer Security Incident Response Team) is frequently used interchangeably to refer to specific response teams. For example, the European Union Agency for Network and Information Security consistently uses the term CERT.

Their competences are defined in Articles 17 and 20 a.c.s. respectively. This relationship is shown in the diagram: [appears in the original version].

CSIRT.CZ is the National CSIRT of the Czech Republic. The Czech National CSIRT is operated on the basis of public contract arranged with the National Security Authority in December 2015. Team CSIRT.CZ fulfills the role of National CERT team as defined in the Act on Cybersecurity. As of 1 January 2011, CSIRT.CZ is administered by the CZ.NIC association.

The first Memorandum about fulfilling the role of National CERT was concluded between the Czech Ministry of Interior and the CZ.NIC association on December 16th 2010. You can find more details about this occasion in the press release at the CZ.NIC website. When National Security Authority took charge of cybersecurity issues in 2011 the memorandum with Ministry of Interior was suppressed by the new memorandum with National Security Authority. First memorandum about fulfilling the role of National CSIRT came into effect on April 1st 2012(About Team). Bigger formal change in the field of cybersecurity is represented since 01.01.2015. A.c.s. defines two high-level teams (governmental CERT and national CERT) and their competences. Governmental CERT is operated by National Cybersecurity Centre which is part of National Security Authority. In august 2015 team CSIRT.CZ was chosen for fulfilling the role of national CERT. As an effect in December 2015 public contract (in czech only) was signed between CZ.NIC association and National Security Authority.

The operator of the national CERT shall act impartially in carrying out the duties imposed on it by a.c.s. and shall coordinate its activities with NÚKIB. The operator of the national CERT may also, in their own name and under their own responsibility, carry out other business activities in the field of cybersecurity not regulated by a.c.s., provided that such activities do not interfere with the performance of the statutory duties. It shall carry out its statutory activities mostly free of charge and shall bear the costs required for the proper and efficient performance of its tasks.

In the meaning of a.c.s., CERT plays a significant role in the process of reporting cybersecurity incidents as outlined in Art. 8. Those incidents that have a significant impact on the continuity of services shall be reported immediately by key service providers to the National Cyber and Information Security (Národní úřad pro kybernetickou a informační bezpečnost, hereinafter: NÚKIB), which acts as the national single point of contact for network and information system security (according to Art. 22 a.c.s.). At the same time, digital service providers or other persons and bodies not listed in Item 3, Art. 8 of a.c.s. report incidents primarily to the national CERT (národní CERT) (a.c.s. provides for reporting to NÚKIB at the same time).

What entity can qualify as a CERT under the Cybersecurity Act? Art. 18 indicates precisely that the operator of a national CERT can only be a legal entity which NÚKIB

has concluded a public law agreement with (pursuant to Art. 163 Art. 4) of the Code of Administrative Procedure for the purpose of cooperation in the field of cybersecurity and for the purpose of providing activities; the precise terms and conditions of the agreements are set out in Art.19 a.c.s.) and which: 1) does not develop or expand their operations contrary to the interests of the Czech Republic within the meaning of the law governing the protection of classified information; 2) has been operating information systems or using services and electronic communications networks for a period of at least 5 years; 3) possesses technical qualification in the area of cybersecurity; 4) is a member of a multinational organisation working in the field of cybersecurity; 5) has no tax arrears registered in the tax registers of the Financial Administration of the Czech Republic, the Customs Administration of the Czech Republic or in the registers of taxes, social security contributions and public health insurance contributions; 6) has not been convicted of an offence referred to in Article 7 of the Act on Criminal Liability of Legal Persons and Proceedings against Them; 7) is not a foreign person within the meaning of any other legal provision; 8) was not set up or established solely for profit; this shall be without prejudice to the ability of the national CERT operator to act in accordance with Section 17 Art. 3.

The applicant shall demonstrate this information by submitting the relevant statements and certificates (regarding financial arrears to the public sector) from the Financial Administration of the Czech Republic and the Customs Administration of the Czech Republic. In order to prove the condition of the possession of a clean criminal record, NÚKIB applies for an extract from the criminal register on the basis of another legal regulation (i.e. Act No. 269/1994 Coll., on the Criminal Register, as Amended, 1994). Following a positive verification, NÚKIB shall publish details of the operator of the National CERT on its website, i.e. their name or surname, their registered office address, their personal identification number, the data box identifier and the address of their website, as well as the contract itself – in the Office Bulletin (except for those parts of the contract that are not allowed for publication on the grounds of other regulations). In the absence of a contract concluded in accordance with Art. 1 or in the event of the termination of the obligation, NÚKIB shall perform the activities of the national CERT.

Item 2 Art. 17 of a.c.s. indicates a broad catalogue of its responsibilities. The National CERT operator: 1) receives notification of contact details from the authorities and persons referred to in Section 3(a), (b) and (h) as well as records and stores such data; 2) receives notifications concerning cybersecurity incidents from the authorities and persons referred to in Section 3 Letters (b) and (h), and records, stores and protects the said data; 3) assesses cybersecurity incidents involving the authorities and persons referred to in Section 3 Letters (b) and (h); 4) provides methodological support, assistance and cooperation to the authorities and persons referred to in Section 3 Letters (a), (b) and (h) in the event of a cybersecurity incident; 5) act as a contact point for the authorities and persons referred to in Section 3 Letters (a), (b) and (h); 6) carries out cybersecurity vulnerability assessments; 7) provides NÚKIB with data on cybersecurity

incidents reported in accordance with Section 8 Item 3, without identifying the notifier; 8) provides the Office, when requested, with the data referred to in Article 16 Sections 5 and 6; 9) acts as a CSIRT in accordance with the relevant European Union regulation 12); 10) informs the competent authority of another Member State, without identifying the notifier, of a cybersecurity incident with a significant impact on the continuity of the provision of a basic or digital service in that Member State and, at the same time, informs the Authority, preserving the security and commercial interests of the notifier; 11) cooperates with CSIRTs in other Member States and receives notifications concerning cybersecurity incidents from authorities and persons not listed in Section 3 and, if its capabilities allow, processes them and provides methodological support, assistance and cooperation to the authorities or persons affected by a given cybersecurity incident.

Government CERT

At the operational level, there exists the Government CERT (GovCERT.CZ) based in Brno. Its main task is to collect reports of cyber incidents from specified entities, analyse them, and provide help (specific provisions are contained in Item 2 Art. 20 a.c.s.). In addition to the responsibilities that are analogous to those of the national CERT (different in terms of the category of entities served), the difference can be seen in the international nature of the responsibilities of the governmental CERT. In accordance with Item 20 Art. 20 of a.c.s., it acts as a CSIRT in accordance with the relevant European Union regulation, i.e. Art. 9 of the EU 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, 2016) and cooperates with other Member States' CERTs. As a rule, the government CERT does not record and store the data it acquires, as the national CERT operator does. It receives and evaluates data from the national CERT operator and from cybersecurity authorities abroad. In the other direction, it provides incident log data to the national CERT operator, authorities with cybersecurity responsibilities abroad and other persons active in the field of cybersecurity in accordance with Art. 9 Section 4. Importantly, it conducts cybersecurity vulnerability assessments (Item j of Art. 20 a.c.s.).

The Act indicates both the inspection related competences held by NÚKIB and the government's inspection related competences in relation to this office (these are outlined in the subsection on NÚKIB).

Article 25 a.c.s. identifies the other entities that commit the offence: a provider of electronic communications services and an entity providing the electronic communications network, an authority or a person providing a basic network.

An electronic communications service provider and an entity providing an electronic communications network commits an offence by: 1) failure, in a state of cyber

emergency or in any other emergency state, to comply with an obligation imposed by the Authority in a decision or measure of a general nature pursuant to Section 13; 2) failure to notify the Authority, without undue delay, of the outcome of the implementation of the preventive measure in accordance with Section 13 Para. 4; 3) fails to submit contact details or changes thereof in accordance with Section 16 Para. 2 Letter a); 4) failure to comply with any of the obligations imposed as a remedy pursuant to Section 24. A body or person providing a network of a significant importance commits an additional offence by: 1) failing to detect cybersecurity incidents under Section 7 Item 3; 2) failing to report a cybersecurity incident under Section 8 Item 1. The administrator of an information or communications system of a critical information infrastructure commits an offence by: 1) in breach of Section 4 Item 2, failing to implement or maintain security measures or security documentation; 2) in breach of Section 4 Item 4, failing to take into account the requirements of security measures when selecting a supplier. An operator of a critical information or communications infrastructure system commits an offence by and the Main Information System Administrator: 1) in breach of Section 4 Item 2 by failing to implement or maintain security measures or security documentation; 2) does not, contrary to Section 4 Para. 4, take into account the requirements of security measures when selecting a supplier or concludes a contract with a supplier contrary to Section 4 Para. 4; 3) as a public authority, in breach of Item 4, fails to classify the cloud computing requested to a security level, does not ensure compliance with the security rules for the provision of cloud computing services or its compliance with availability conditions, or concludes a contract with a cloud computing service provider in breach of Item 4; 4) fails to inform the body providing an electronic communications network in accordance with § 4a Para. 2; 5) does not communicate data, operational data and information in accordance with § 6a Para. 2; 6) does not transmit data, traffic data and information in accordance with Section 6a Para. 3; 7) not destroy copies of the data, traffic data and information referred to in Section 6a Para. 3; 8) does not enable the administrator to monitor the progress of the destruction of data, traffic data and the information referred to in Art. 6a Para. 3. The operator of the main information system commits an offence by: […]. The administrator of a core service information system commits an offence if: […]. Basic Services Information System Operator. A basic service provider commits an offence by: 1) as a public authority, in breach of Item 4(5), a failure to classify an on-demand cloud computing service as a security service, a failure to ensure compliance with the security rules for the provision of cloud computing services or compliance with availability conditions, or enters into a contract with a cloud computing service provider in breach of Item 4; 2) failure to inform the administrator or the operator of an IT system of the provision of a basic service in accordance with § 4a Para. 3; 3) failure to notify of significant impact on the continuity of a basic service in accordance with § 8 Para. 1, 4 or 8. A digital service provider commits an offence by a failure to appoint a representative in accordance with Section 3a Para. 1. A manufacturer or a supplier of products, services or processes who is issuing an EU declaration of conformity commits an offence by issuing an EU Declaration of Conformity when the conditions as set out

in the Cybersecurity Act are not met for it being issued. A holder of a European Cybersecurity Certificate commits an offence by failing to inform the relevant conformity assessment bodies of any vulnerabilities or irregularities that are subsequently identified. A legal or natural person commits an offence by: 1) an illegitimate use of a mark or designation of the European Cybersecurity Certification Scheme, a European Cybersecurity Certificate, an EU Declaration of Conformity or any other document under the Cybersecurity Act; 2) forging or altering a European Cybersecurity Certificate, an EU Declaration of Conformity or any other document under the Cybersecurity Act; 3) conducts conformity assessment activities under the Cybersecurity Act 17) to an assurance level of "high", even though it is not authorised to do so under Art. 56 Para. 6 of the Cybersecurity Act. An individual also commits an offence by breaching the duty referred to in Para. 10 Item 1 a.c.s.

Conclusion

Virtual reality and the global information space, including the digital space, have brought with them a new post-modern quality of life, which, unfortunately, carries certain problems. The deeper one enters the ICT space, the more risk there is of encountering dangerous phenomena and events associated with that domain. New risks emerge in line with constant progress, also in the area of cyberspace. One of the features of cyberspace is its massive scale, both in terms of potential sources of information and their recipients. However, the universality and global nature of the modern information sphere generate a large number of potential threats. Examples of such threats include technical interference with the proper functioning of cyberspace, but also interference with the quality of the information itself, through the dissemination of fake news, the manipulation of information, or the spreading of ideological propaganda. Stable cyberspace guarantees the proper functioning of the institutional structures of the state, as well as of the critical infrastructure (Drabik, 2022: 22-23).

Information space is the natural environment of humans of the digital age. The free circulation of information is the result of civilisational development, but in addition to all its cognitive benefits, it carries various threats, including the risk of spreading disinformation. These threats distort the clarity of the message and make it impossible for the recipient to judge the veracity of the content. Measures are needed to ensure the credibility of information transmission channels in order to expose disinformation and combat it by institutions responsible for the protection of society. Also, users need to be equipped with the right tools to recognise and combat this phenomenon (Gergelewicz, 2022: 83). To meet the expectations of society related to the area of cybersecurity, it is important to limit not only criminal activity but also other behaviour that is antisocial in nature. Based on an objective assessment of threats, it should be pointed out that a similar level of anxiety is experienced by people who fear burglary or theft, and people who experience aggression via modern communication and information technologies (Pieczywok, 2019: 63).

Universal access to the Internet and the digitalisation of the social sphere of life has made cyberspace an arena of conflict between states, as well as blocs of states in intelligence wars. One aspect of such conflicts is information warfare. The greater the digital competence gaps in society, the greater the efficiency of such warfare. This applies both to the susceptibility of society to various types of disinformation and the failure to follow the principles of security (Kaczmarek, 2022: 36). Ensuring the security of the state in cyberspace should be the priority of the services responsible for protecting strategic information systems (Kostrubiec, 2022a: 16). These systems are

responsible for the stability of the state and its economy and must therefore be properly protected. They also play a very important role in society, and, therefore, their reliability and security must be a priority for the entities, both from the public and private sectors, responsible for the operation of such systems.

Since an appropriate level of protection of information systems must be ensured, restrictions on individual freedoms and rights in cyberspace are permissible in certain cases, provided that such protection cannot otherwise be ensured (Czuryk, 2022a: 34). Cybersecurity measures taken in the public interest may, therefore, in some cases take precedence over other values protected under the constitution (including human rights and freedoms). However, this should only be resorted to in exceptional cases, and such broad interpretation should not be applied to provisions that give primacy to state cybersecurity in the event of a conflict between constitutional values. Any doubts should normally be interpreted in favour of individual freedoms and rights, preventing interference with the provisions related to cybersecurity in that sphere (Karpiuk, 2022d: 410-411).

References

Banaszak, B. (2009) *Konstytucja Rzeczypospolitej Polskiej, Komentarz* (Warsaw: C.H. Beck).

Bencsik, A. & Karpiuk, M. (2023) Cybersecurity in Hungary and Poland. Military aspects, *Cybersecurity and Law*, 9(1), pp. 82-94.

Bokšová, J. & Bokša, M. (2018) Digitalization of Public Administration and Services, *Digital Czechia in Digital Europe*, available at: https://www.researchgate.net/publication/348900018_Digital_Czechia_in_Digital_Europe (September 10, 2022).

Chałubińska-Jentkiewicz, K. & Brzostek, A. (2021) *Strategie cyberbezpieczeństwa współczesnego świata* (Warsaw: TWO).

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

Csányi, C. (2021) Current national security challenges affecting Hungary and possible legal responses to them, *Hungarian Law*, 7-8, pp. 474-480.

CSIRT.SK (2022), available at: https://www.csirt.gov.sk/index.html?csrt=8058637170998233146 (November 29, 2022).

Cyber Defence 24 (2018) *Czeska armia stawia na cyberbezpieczeństwo*, available at: https://cyberdefence24.pl/armia-i-sluzby/czeska-armia-stawia-na-cyberbezpieczenstwo (September 1, 2022).

Czaputowicz, J. (2008) *Teorie stosunków międzynarodowych. Krytyka i systematyzacja* (Warszawa: Wydawnictwa Naukowe PWN).

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

Czuryk, M. (2021) Cybersecurity as a premise to introduce a state of exception, *Cybersecurity and Law*, 6(2), pp. 83-90, https://doi.org/10.35467/cal/146466.

Czuryk, M. (2022a) Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues, *Studia Iuridica Lublinensia*, 31(3), pp. 31-43, http://dx.doi.org/10.17951/sil.2022.31.3.31-43.

Czuryk, M. (2022a) Special rules of remuneration for individuals performing cybersecurity tasks *Cybersecurity and Law*, 8(2), pp. 105-112, https://doi.org/10.35467/cal/157128.

Czuryk, M. (2022b) Supervision and Inspection in the Field of Cybersecurity, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 111-119, https://doi.org/10.4335/2022.1.

Czuryk, M., Dunaj, K., Karpiuk, M. & Prokop, K. (2016) *Prawo zarządzania kryzysowego. Zarys systemu* (Olsztyn: UWM).

Drabik, K. (2022) Cyberspace in a risk society, *Cybersecurity and Law*, 7(1), pp. 17-26, https://doi.org/10.35467/cal/151808.

ENISA (2012) *Deployment of Baseline Capabilities of National/Governmental CERTs*, available at: https://www.enisa.europa.eu/publications/updated-recommendations-2012/@@download/fullReport (September 3, 2022).

European Commission (2022) *Digital Economy and Society Index (DESI) 2022, Czechia*, available at: https://ec.europa.eu/digital-agenda/en/scoreboard/czech- republic (October 1, 2022).

Expats CZ (2022) *Russian hackers target Czech websites in a series of cyberattacks*, available at: https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks (September 1, 2022).

Fekete-Krydis, K. & Lázár, B. (2020) Military dimensions of cyber defence, *Military Defence Review*, 143(3), pp. 44-54.

Firniksz, J. (2021) Rankings – A New Regulatory Issue In The Age Of Platforms And Information Supply, In: Valentiny, P., Antal-Pomázi, K., Nagy, C. & Berezvai, Z. (eds.) *Competition and Regulation* (Budapest: KRTK Institute of Economics), pp. 165-199, available at: https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf (July 31, 2022).

Gapiński, K. (2015) *Czesi podpisują memorandum z NATO i rozwijają europejską współpracę w zakresie cyberbezpieczeństwa*, available at: https://pulaski.pl/experts-commentary-the-world-is-mobilizing-in-response-to-the-threat-posed-by-putins-russia-is-russian-opposition-playing-its-full-part-robert-pszczel/ (September 2, 2022).

Gergelewicz, T. (2022) Obszary budowania odporności na dezinformację jako element bezpieczeństwa infosfery, *Cybersecurity and Law*, 7(1), pp. 72-84, https://doi.org/10.35467/cal/151814.

Gizicki, W. (2013) *A security community: Poland and her Visegrad allies: the Czech Republic, Hungary and Slovakia* (Lublin: Catholic University of Lublin Publishing House).

Górka, M. (2019) *Istota bezpieczeństwa cybernetycznego w polityce państw Grupy Wyszehradzkiej w latach 2013-2017* (Warsaw: Difin).

Hoffman, I. (2021) Cybersecurity and public administration in the time of corona(virus) – in the light of the recent Hungarian challenges, *Cybersecurity and Law*, 5(1), pp. 145-158, https://doi.org/10.35467/cal/142201.

Hoffman, I. & Karpiuk, M. (2022a) E-administration in Polish and Hungarian Municipalities – a Comparative Analysis of the Regulatory Issues, *Lex Localis – Journal of Local Self-Government*, 20(3), pp. 617-640, https://doi.org/10.4335/20.3.617-640(2022).

Hoffman, I. & Karpiuk, M. (2022b) The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary, *Cybersecurity and Law*, 7(1), pp. 171-190, https://doi.org/10.35467/cal/151826.

Kaczmarek, K. (2019) Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii, *Cybersecurity and Law*, (1)1, pp. 143-157, https://doi.org/10.35467/cal/133778.

Kaczmarek, K. (2022) Appealing to compassion as an element of Russia's hybrid warfare against the West, *Cybersecurity and Law*, 7(1), pp. 51-60, https://doi.org/10.35467/cal/151812.

Kaczmarek, K. (2022) Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 29-37, https://doi.org/10.4335/2022.1.

Karpiuk, M. (2020) The obligations of public entities within the national cybersecurity system, *Cybersecurity and Law*, 4(2), pp. 57-72, https://doi.org/10.35467/cal/133971.

Karpiuk, M. (2021a) Cybersecurity as an element in the planning activities of public administration, *Cybersecurity and Law*, 5(1), pp. 45-52, https://doi.org/10.35467/cal/142179.

Karpiuk, M. (2021b) 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.

Karpiuk, M. (2021c) 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. (2022a) Cybersecurity-related responsibilities of the minister competent for computerization, *Cybersecurity and Law*, 8(2), pp. 17-26, https://doi.org/10.35467/cal/157120.

Karpiuk, M. (2022b) Tasks of the Minister of National Defense in the area of cybersecurity, *Cybersecurity and Law*, 7(1), pp. 85-94, https://doi.org/10.35467/cal/151816.

Karpiuk, M. (2022c) The Competence of the Internal Security Agency in Protecting the Security of Communication and Information Systems and Networks of Public Administration Authorities, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 69-78, https://doi.org/10.4335/2022.1.

Karpiuk, M. (2022d) The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights, *Przegląd Prawa Konstytucyjnego*, 3(67), pp. 401-412, https://doi.org/10.15804/ppk.2022.03.30.

Karpiuk, M. & Kelemen, M. (2022) Cybersecurity in civil aviation in Poland and Slovakia, *Cybersecurity and Law*, 8(2), pp. 70-83, https://doi.org/10.35467/cal/157125.

Kelemen, M. (2014) *Selected problems of protection of persons, property and securing of other protected interests in security sectors* (Bratislava: VEDA publishing house SAV).

Kelemen, M. (2017) *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests* (Banská Bystrica: Belianum. Matej Bel University Press).

Kelemen, M., Polishchuk, V., Gavurová, B., Andoga, R., Szabo, S., Yang, W., Christodoulakis, J., Gera, M., Kozuba, J., Kaľavský, P. & Antoško, M. (2020) Educational Model for Evaluation of Airport NIS Security for Safe and Sustainable Air Transport, *Sustainability*, 12(16), pp. 1-20, https://doi.org/10.3390/su12166352.

Kerekes, L. (2021) "Waiting for Godot..." Challenges of codifying a unified convention against cybercrime, *Debrecen Legal Workshop*, 3-4, pp. 32-41.

Kostrubiec, J. (2022a) Cybersecurity System in Poland, Selected Legal Issues, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 7-17, https://doi.org/10.4335/2022.1.

Kostrubiec, J. (2022b) The position of the Computer Security Incidents Response Teams in the national cybersecurity system, *Cybersecurity and Law*, 8(2), pp. 27-35, https://doi.org/10.35467/cal/157121.

Kotowski, W. (2012) *Ustawa o Policji, Komentarz* (Warsaw: Wolters Kluwer).

Krasznay, C. & Muha, L. (2013) Cyber defence in Hungary: a blessing or a curse?, *HWSW Online IT News Magazine* (May 3, 2013), available at: https://www.hwsw.hu/hirek/50206/kibervedelem-biztonsag-jog-torveny.html (May 16, 2023).

Krupa, Ł. (2022) Money laundering and cybercrime, *Cybersecurity and Law*, 8(2), pp. 160-165, https://doi.org/10.35467/cal/157180.

Lebowa, D. (2022) Procedure for the Identification of an Operator of Essential Services under the Act on the National Cybersecurity System, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 101-110, https://doi.org/10.4335/2022.1.

Madarász, L. (2003) *Methodology of situational management and its applications* (Košice: ELFA TU KE).

Marczyk, M. & Pilarski, G. (2021) Internet rzeczy i jego wykorzystanie w cyberprzestrzeni jako nowym środowisku walki, In: Marczyk, M., Stolarz, M. & Terebiński, B. (eds.) *Działania hybrydowe a bezpieczeństwo sieci i systemów teleinformatycznych w SZ RP – wybrane aspekty* (Warszawa: ASzWoj), pp. 303- 330.

Mašlanyová, D., Klátik, J. & Strémy, T. (2016) *Substantive criminal law: general and special* (Pilsen: Vydavatelství a nakladatelství Aleš Čeněk).

Mezei, K. (2019) Current issues of the domestic regulation of cybercrimes, *Hungarian Law*, 66(5), pp. 305-314.

Milik, P. (2021) Uwarunkowania globalne cyberbezpieczeństwa, In: Chałubińska-Jentkiewicz, K. & Brzostek, A. (eds.) *Modele rozwiązań prawnych w systemie cyberbezpieczeństwa RP. Rekomendacje* (Warsaw: TWO), pp. 11-48.

Ministry of Defence & Armed Forces of the Czech Republic (2020) *Cyber Forces Command*, available at: https://www.army.cz/en/armed-forces/organisational-structure/cyb/cyber-forces-command-218593/ (September 1, 2022).

Ministry of Foreign Affairs of the Czech Republic (2015) *Security Strategy of the Czech Republic 2015*, available at: https://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf (September 1, 2022).

Ministry of Foreign Affairs of the Czech Republic (2015) *Updated Security Strategy of the Czech Republic*, available at: https://www.mzv.cz/jnp/en/issues_and_press/archive/events_and_issues/x2015/x2015_02_05_update_of_security_strategy.html (October 1, 2022).

Ministry of industry and trade, Odbor komunikace (2022) *Czech Republic became a member of the Council of the International Telecommunication Union, which decides on the development of communication technology*, available at: https://www.mpo.cz/en/guidepost/for-the-media/press-releases/czech-republic-became-a-member-of-the-council-of-the-international-telecommunication-union--which-decides-on-the-development-of-communication-technolo--270270/ (October 1, 2022).

Müller, A.W. & Müller-Stewens, G. (2009) *Strategic Foresight: Trend- und Zukunftsforschung in Unternehmen - Instrumente, Prozesse, Fallstudien* (Stuttgard: Schäffer-Poeschel).

National Cyber and Information Security Agency (2022) *Provided Services*, available at: https://nukib.cz/en/cyber-security/government-cert/provided-services/ (September 21, 2022).

National Security Office (2021) *Report on cyber security in the Slovak Republic in 2021*, available at: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf (November 29, 2022).

Nečas, P. & Kelemen, M. (2010) *War on insecurity: calling for effective strategy*! (Kiev: The Center of Educational Literature).

Nyáry, G. (2020) Cyber diplomacy: power, politics and technology in the fifth dimension of geopolitics, In: Török, B. (ed.) *Information and cybersecurity* (Budapest: Ludovika University Publishing House), pp. 165-199.

Pawelec, K. (2022) Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji, *Cybersecurity and Law*, 7(1), pp. 130-141, https://doi.org/10.35467/cal/151820.

Pawlikowska, I. (2004) Bezpieczeństwo jako cel polityki zagranicznej państwa, In: Zięba, R. (ed.) *Wstęp do teorii polityki zagranicznej państwa* (Toruń: Adam Marszałek), pp. 61–63.

Pelc, P. (2022) The Role of Cybersecurity in the Public Sphere – The European Dimension. Financial Institutions, In: Chałubińska-Jentkiewicz, K. & Hoffman, I. (eds.) *The Role of Cybersecurity in the Public Sphere – The European Dimension* (Maribor: Lex Localis Press), pp. 59-68, https://doi.org/10.4335/2022.2.

Pieczywok, A. (2019) The use of selected social concepts and educational programmes in counteracting cyberspace threats, *Cybersecurity and Law*, 2(2), pp. 61-74.

Pieczywok, A., Kościelny, M. & Wasilewski, S. (2021) Kształtowanie bezpieczeństwa środowiskowego i w cyberprzestrzeni – porównanie zagrożeń, *Cybersecurity and Law*, 6(2), pp. 69-82.

Portal VS (2022) *Fields of study*, available at: https://www.portalvs.sk/sk/studijne-odbory/zobrazit/80301 (November 22, 2022).

Reuters (2022) *Czech capital Prague, Labour Ministry face cyberattacks*, available at: https://www.reuters.com/world/czech-capital-prague-labour-ministry-face-cyber-attacks-2021-03-05/ (September 11, 2022).

Rezek, T. (2012) Cyberbezpieczeństwo Republiki Czeskiej, In: Świątkowska, J. (ed.) *Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje* (Kraków: Wydawnictwo Instytutu Kościuszki), pp. 31–42.

Romaniuk, P. (2022) Administrative and legal obligations of the auditee in connection with the performance of an audit task in local government units, *Cybersecurity and Law*, 7(1), pp. 191-201, https://doi.org/10.35467/cal/151827.

Security (2020) *Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak*, available at: https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak (October 1, 2022).

Security information service (2022) *Who we are*, available at: https://www.bis.cz/about-us/ (September 2, 2022).

Slovak Liaison Office for Research and Development (2022), available at: https://www.slord.sk/about-us/?lang=en (October 14, 2022).

Slov-Lex (2017) *Comments raised within the interdepartmental comment procedure*, available at: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/407 (November 22, 2022).

Slov-Lex (2017) *Explanatory report on the draft law on cyber security*, available at: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-407 (November 29, 2022).

Stefanowicz, J. (1984) *Bezpieczeństwo współczesnych państw* (Warszawa: Instytut Wydawniczy Pax).

Stolarz, M. (2021) Cyberprzestrzeń w wojnie hybrydowej, In: Marczyk, M., Stolarz, M. & Terebiński, B. (eds.) *Działania hybrydowe a bezpieczeństwo sieci i systemów teleinformatycznych w SZ RP – wybrane aspekty* (Warszawa: ASzWoj), pp. 13-51.

Szathmáry, Z. (2021) Legitimate defence in cyberspace, *Hungarian Law*, 68(11), pp. 642-650.

Tóth, A. (2016) Resolutions and agreements following the Prague NATO Summit on the modernisation of the command and control system and the development of joint operational capability, *Military Engineer*, 11(3), pp. 214-220.

Tóth, A. (2017) The foundations of European regulation of network and information systems security, *Infocommunication and Law*, 14(1), pp. 16-24.

Tóth, T. (2018) Introducing the NATO Cyber Defence Centre of Excellence, *National Security Review*, 6(4), pp. 48-62.

Tyrawa, D. (2022) The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity, In: Karpiuk, M. & Kostrubiec, J. (eds.) *The Public Dimension of Cybersecurity* (Maribor: Lex Localis Press), pp. 19-28, https://doi.org/10.4335/2022.1.

Wasiuta, M. (2021) *Czeskie zmagania z e-administracją w dobie pandemii*, available at: https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2021-09-08/czeskie-zmagania-z-e-administracja-w-dobie-pandemii (September 5, 2022).

Włodyka, E. (2022) Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa, *Cybersecurity and Law*, 7(1), pp. 202-219, https://doi.org/10.35467/cal/151828.

Zdzikot, T. (2022) The Role of the State and Public Administration in the Cybersecurity System, In: Chałubińska-Jentkiewicz, K. & Hoffman, I. (eds.) *The Role of Cybersecurity in the Public Sphere – The European Dimension* (Maribor: Lex Localis Press), pp. 37-46, https://doi.org/10.4335/2022.2.

Zięba, R. (2008) Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego, In: Zięba, R. (ed.) *Bezpieczeństwo międzynarodowe po zimnej wojnie* (Warsaw: Wydawnictwa Akademickie i Profesjonalne), pp. 15-39.

Institute for Local Self-Government Maribor

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