Cybersecurity Policy

KATARZYNA CHAŁUBIŃSKA-JENTKIEWICZ

Abstract In the contemporary digital world, cybersecurity is one of the most fundamental issues. Cybersecurity management in business activities and the safe operation of public sector institutions constitutes the key element to create conditions for an efficient and safe functioning of the state. The effectiveness of the introduced regulations governing cyberspace largely depends on the efficient operation of organisational units and institutions responsible for combating and counteracting cybercrime. New entities dealing with the protection of cyberspace have recently been established, and they also cooperate with similar entities operating at international level (Szczepaniuk, 2016: 135). As regards cybersecurity management, attention should also be paid to elements comprising information security – the set of rules, practices and procedures, and the types of threats identified in cyberspace.

Keywords: • cybersecurity • cybersecurity policy • information security

CORRESPONDENCE ADDRESS: Katarzyna Chałubińska-Jentkiewicz, Ph.D., Dr. Habil., Associate Professor, War Studies University, Law Institute, Aleja Generała Antoniego Chruściela „Montera" 103, 00-910 Warsaw, Poland, email: k.jentkiewicz@akademia.mil.pl.

https://doi.org/10.4335/2021.5 ISBN 978-961-7124-03-3 (PDF)
Available online at http://www.lex-localis.press.

1 Competent authorities for cybersecurity

As already mentioned in the preceding chapter, in the Republic of Poland, the tasks in the area of cybersecurity, just like all other security-related tasks, are performed by public authorities and subordinated administration authorities. According to the constitutional division, public authorities are those which hold legislative, judicial, and executive powers (Article 10 (1) of the Constitution of the Republic of Poland).

These functions arise from general public tasks for ensuring national security. W. Kitler cites, inter alia, the protection of the constitutional order, understood as the activities of state authorities and institutions, and the system of legal rules guaranteeing the continuity of the constitutional state system, including the protection of the state as a legal and political organisation, as well as the protection of freedom and human and civil rights, and the protection of classified information and personal data, the protection of the life and health of the people, and of goods and the environment, from the negative effects of human activities, technical failures and natural forces (Kitler, 2011). It should be noted that all these values can be affected by the risks arising from the use of cyberspace. The role of the legislative authority, which includes the Sejm (the lower House of the Polish Parliament) and the Senate, in the field of cybersecurity mainly arises from its system-forming functions, including legislation. This encompasses legislation and the definition of the main objectives of the state's activities, which is related to the effectiveness of the Polish legal system and the activities carried out by administrative authorities (Chałubińska-Jentkiewicz, 2014: 25).

Public authorities also include the judiciary. Its main tasks, which it also carries out within the ambit of cybersecurity, include the administration of criminal justice. These often relate to national security in general, as well as to its cross-sectoral field, that is to say, cybersecurity, with its normative rules of conduct (Chałubińska-Jentkiewicz, 2014: 25).

However, the key role in the field of cybersecurity is played by the executive branch. Its competences involve managing cybersecurity through influencing the behaviour of others and supervising their actions, but also by taking specific measures, having the tools and managing the assets related to the achievement of its objectives (Kitler 2011: 26).

The Constitution of the Republic of Poland states that executive power in Poland is held by the President and the Council of Ministers (Article 10 (2) of the Constitution). The President of the Republic of Poland shall ensure the observance of the Constitution, safeguard the sovereignty and security of the state, as well as the inviolability and integrity of its territory (Article 126 (2) of the Constitution of the Republic of Poland). This provision is general, but a more specific function follows from Article 230 (1), which states that "in the case of threats to the constitutional order of the state, to citizen security or public order, the President of the Republic of Poland may introduce for a definite period no longer than 90 days, a state of emergency in a part of or upon the whole territory of the State. This is all the more important, as, under the State of Emergency Act, these

threats can be caused by actions in cyberspace, as laid down in Article 2 (1) of the Act of 21 June 2002 on the State of Emergency (consolidated text, Polish Journal of Laws of 2016, item 886, as amended).

A special role in ensuring the security of cyberspace lies with the Council of Ministers, consisting of the Prime Minister and ministers. As noted by W. Kitler, the Council of Ministers is the "leader" of the public administration (Kitler: 2011), as it is responsible for implementing laws and controlling and coordinating the activities of government administration authorities. The Council of Ministers is responsible for the state's external security, internal security, and public order, which includes the implementation of cybersecurity tasks. Other tasks related to cybersecurity include crisis management on the territory of the Republic of Poland, actions for the protection of critical infrastructure, and, in situations of special threats, including those arising from cyberspace, which cannot be removed by ordinary constitutional means, the Council of Ministers may adopt a Resolution to request the President to impose a state of emergency or martial law, and in certain cases it may itself impose a state of natural disaster (Articles 228-232 of the Constitution of the Republic of Poland).

The leading role in the Council of Ministers is played by the Prime Minister, who presides over the Council of Ministers, and who is responsible for the protection of the cyberspace on the territory of Poland, and performs related tasks through: 1) the Ministry of the Interior and Administration; 2) the Ministry of Digital Affairs, 3) the Ministry of National Defence (MON); 4) the Head of the Internal Security Agency (ISA), 3) and the Head of the Military Counterintelligence Service (MCS)[1].

The second authority of the Council of Ministers is made up of the ministers themselves, who head individual departments. They define the principles, methods, and ways of performing public tasks, in the offices and organisational units subsidiary to them (Chałubińska-Jentkiewicz, 2014: 27).

Cybersecurity as a cross-sectoral field involves all administrative authorities. Public tasks focused on this field are performed by various types of state entities, guards, services, and inspections subordinate to the Prime Minister or individual Ministers (Chałubińska-Jentkiewicz 2014: 27).

As regards entities dealing with the issues of compliance with law in cyberspace, it is worth mentioning the entities which have limited powers in this area, and are related to the protection of personal data, classified information and the protection of the telecommunications markets. These authorities include: the President of the Personal

[1] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

Data Protection Office, the President of the Office of Electronic Communications, and the President of the Office of Competition and Consumer Protection[2].

The President of the Personal Data Protection Office is a competent authority for personal data protection affairs. The authority's obligations include most of all control over the compliance of data processing with personal data protection laws. In addition, the main tasks of the President of the Personal Data Protection Office include issuing administrative decisions and examining complaints in matters concerning compliance with personal data protection laws, maintaining data set registers, and providing information on the registered sets, issuing opinions on bills and regulations related to personal data protection[3].

The scope of activities performed by the President of the Office of Electronic Communications, as laid down in the Telecommunications Law of 16 July 2004 (consolidated text, Polish Journal of Laws of 2017, item 1907, as amended), includes tasks entailing the regulation and control of telecommunications market services. The authority may control compliance with decisions and orders in the scope of telecommunications. Taking into account the aforementioned powers, it can be stated that the Office of Electronic Communications may be regarded as a competent authority in matters concerning the processing of transmission data by the operators of public telecommunications networks or providers of publicly available services[4].

The President of the Office of Competition and Consumer Protection oversees compliance with the law in cyberspace only to a limited extent. The main powers of the authority include conducting proceedings and issuing decisions in matters concerning practices which are in breach of collective consumer interests. The detailed scope of the powers entrusted to the said authority is defined in the Act of 16 February 2007 on Competition and Consumer Protection (consolidated text, Polish Journal of Laws of 2017, item 229, as amended). It should be mentioned that a vital extension of the powers of the Office of Competition and Consumer Protection is the possibility to institute ex officio proceedings in the event of a collective breach of Internet users' interests (Wojciechowska-Filipek, Ciekanowski, 2016: 36).

In today's hugely computerised reality, in addition to the operations of the abovementioned administration authorities, intended to provide the security of various resources, there is a growing need to provide protection in the technical aspect. Such function is performed by CERTs. CERTs are often entities which do not have a separate legal personality. They usually run activities as part of other organisations or companies, and are small teams of several, or a dozen or so people operating within the structures of larger entities. In most cases, the institution comprising a CERT has substantial

[2] The Office of Competition and Consumer Protection www.uokik.gov.pl.
[3] Ibidem.
[4] Office of Electronic Communications www.uke.gov.pl.

communication and information resources (e.g. operators) or a significant responsibility (e.g. state structures). CERT is an abbreviation for a Computer Emergency Response Team. "Computer emergency" means every incident which compromises or threatens to compromise the infrastructure for which a given CERT is responsible (Werner, 2014: 36).

There are security teams (another name for CERT) operating within the structures of Internet providers, government CERTs which protect the state information infrastructure, military CERTs, academic CERTs, or CERTs in large companies (usually from the IT sector). This diversity does not change the fact that all such entities deal with the same issues: hacking, attacks, computer fraud, and their objective is to provide the safety of the infrastructure area under their management. If an incident occurs, response teams initiate procedures aimed at eliminating or at least mitigating the threat. It is often possible thanks to long-standing cooperation and an extensive network of contacts between such teams as the police, governmental and financial institutions, and telecommunications operators. As the Internet does not recognise state boundaries in their traditional sense, cooperation between such teams is one of the key aspects of their operations (Werner, 2014: 36).

In most European states, there is at least one national-level CERT which constitutes a point of contact for a given country. The first team of this type in Poland was CERT Polska, established in 1996, conducting activities within the structure of the research institute of the Research and Academic Computer Network, and handling incidents related to ICT security on the Polish Internet. Government CERT is responsible for the protection of the public administration network[5]. There are also CERTs established within the organisational structures of major Polish telecommunications operators, and a military CERT (Werner 2014: 37).

The most important bodies responsible for cybersecurity include the Internal Security Agency (the ISA), whose Head reports directly to the Prime Minister. The ISA is competent for the internal security of the state and its constitutional order, pursuant to Article 1 of the Act of 24 May 2002 on the Internal Security Agency and on the Intelligence Service (consolidated text, Polish Journal of Laws of 2017, item 1920, as amended). These responsibilities also include cybersecurity, including tasks which the ISA performs through the Department of Information and Communication Security ("DBTI") and the Department of Classified Information Protection (Chałubińska-Jentkiewicz, 2014: 27). The Governmental Computer Security Incident Response Team, CERT.GOV.PL, was established in February 2008, and it plays the role of an IT division at the ISA operating within the structures of the DBTI.

The mission of the CERT.GOV.PL is 1) to cooperate with domestic organisations, institutions and ministry entities in the sphere of cyberspace protection; 2) to synchronise the exchange of information between entities in this respect; 3) to outline the cyberthreat protection policy, 3) to respond to incidents interfering with ICT security, with particular

[5] www.cert.gov.pl.

attention to the critical infrastructure of the state; 5) to raise the awareness of computer threats and provide related training, 6) to represent the Republic of Poland in international relations (in the scope of military cooperation, in consultation with the Computer Incident Response System Coordination Centre within the Ministry of National Defence); 7) to acquire knowledge on the threats to, and the security status of, critical communication and information infrastructure; 8) to prepare periodic reports as part of the state's ICT security[6].

The tasks of the Head of the ISA (and the Head of the MCS in the military domain), performed by the CERT.GOV.PL team in the scope of protecting critical communication and information infrastructure, include such activities as: 1) preparing analyses in the field of the state's critical communication and information infrastructure; 2) creating and managing the system for the coordination of counteracting, combating and responding to threats and attacks on the state's cyberspace, including management of the register of the state's critical communication and information infrastructure, and the Head of the ISA should make an entry in the said register, ex officio, for government and local government administration authorities, and state-owned legal persons and, upon request, for enterprises and community organisations performing public tasks; 3) collecting and processing information in the register and providing access to such information; 4) cooperating on an international scale as part of the protection of the state's critical communication and information infrastructure; 5) controlling the protection of communication and information systems or networks listed in the register; 6) the Head of the ISA, as part of international relations and cooperation, plays the role of a national authority competent for the protection of the state's critical infrastructure[7].

Thanks to the cooperation between DPTI and the CERT Polska operating within the structures of NASK (coordination Team of the Research and Academic Computer Network at the University of Warsaw), the ARAKIS-GOV[8] system was developed. It is a system intended for providing early warnings about Internet threats, which supports the state administration in respect of the protection of its communication and information resources.

ARAKIS-GOV is not a traditional security system, and in no respect can it replace the role of standard network protection systems, like firewalls, anti-virus software or IDS/IPS. The functioning of this system consists in the aggregation of information about network threats based on network traffic surveillance (with the use of distributed probes) and information from external sources. An unique feature of the ARAKIS-GOV system is the fact that it does not observe the contents of information exchanged via the

[6] The Governmental Computer Security Incident Response Team CERT.GOV.PL http://abw.gov.pl/, http://www.cert.gov.pl/portal/cer.
[7] The Government Cyberspace Protection Programme of the Republic of Poland for 2009-2011. Principles, Warsaw, March 2009. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_ Security_Strategy.pdf.
[8] http://www.cert.gov.pl.

institution's internal network under protection, on the Internet side. Currently the system sensors are located in over 60 central agencies and local government entities, i.a., 16 ministries, 11 local government authorities, and other entities including the Central Anti-Corruption Bureau, the National Security Bureau, the Social Security Institution or the Senate of the Republic of Poland (Wojciechowsla-Filipek, Ciakanowski, 2016: 225).

Poland established numerous institutions and put forward initiatives aimed at combating cyberterrorism. The most important ones are 1) HoneySpider Network – a project developed with a view to building and improving applications responsible for detecting attacks against web browsers, e.g. drive-by download; 2) ABUSE-FORUM – an informal group of experts who represent major Polish Internet providers, telecommunications operators, web portals and public administration authorities; 3) WOMBAT – it is a project aimed at developing an international application which allows the monitoring and detection of network threats; 4) FISHA – a system allowing the creation of an European information exchange and access programme, to provide early detection of threats resulting from the use of communication and information networks[9].

However, the key function in providing cybersecurity is performed by the Commander-in-Chief of Police, an authority subordinate to the Minister of the Interior and Administration. Crime in the cyberspace is the focus of operations performed by the Cybercrime Department of the Criminal Bureau of the National Police Headquarters, responsible for: 1) out-of-court cooperation with third-party entities in the scope of investigations involving telecommunications and ICT services; 2) continuous monitoring and analysis of threats on the Internet as part of their operational work methods, 3) providing technical support to units performing tasks in the sphere of fighting computer crime[10].

According to the order of battle, the main tasks entrusted to structures responsible for combating cybercrime include: 1) using the advanced technology units within the division, 2) defining the cybercrime threat areas to be monitored; 3) operational techniques which provide technical support and tools for combating cybercrime to the substantive departments of the criminal investigation division and the Central Bureau of Investigation, 4) performing operation and investigation activities in line with the competence of substantive departments of the criminal investigation division and the Central Bureau of Investigation (depending on the area being monitored), 5) substantive responsibility of the organisational units within the Criminal Bureau of the National Police Headquarters for the coordination of operational and investigative works in individual areas; 6) monitoring individual areas of Internet threats in defined units

[9] The Government Cyberspace Protection Programme of the Republic of Poland for 2009-2011. Principles, Warsaw, March 2009. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_ Security_Strategy.pdf.
[10] Organisational order No. 31/14 dated 26 June 2014 on the organisational and personnel changes at the National Police Headquarters.

responsible for operational methods at the Provincial Police Headquarters, without fragmenting forces or resources; 7) identifying, verifying and introducing advanced technical support tools for combating cybercrime (Paprzycki, Rau, 2009: 171).

In line with the "Concept of technical support for combating cybercrime" of 17 February 2007, approved by the Commander-in-Chief of Police, the Criminal Bureau of the National Police Headquarters has gained an Advanced Technology Section (ZT) at the Advanced Technology Department as of June 2007. It is mainly responsible for monitoring threats related to cybercrime, identifying, verifying and implementing advanced technical support tools for combating cybercrime, providing advice on complex issues related to the matter in question, and implementing Internet arrangements. Furthermore, the tasks of the Section also include participation in European and other international initiatives related to combating cybercrime (Paprzycki, Rau, 2009: 171-172). At the same time, advanced technology units were established within the Departments of Operational Methods in the Provincial Police Headquarters, whose main task was to support the substantive department of criminal investigation divisions, by applying expertise and IT tools with a view to combating the identified areas of threats.

As regards combating cybercrime, the following areas were identified and are subject to monitoring: 1) child pornography, mainly in P2P networks; 2) dissemination of illegal content; 3) disclosure of information concerning the location of identity data; 4) obtaining credit card numbers by false pretences; 5) breach of copyright, especially in P2P networks; 6) surveillance of "hooligan" circles[11].

In order to ensure the proper fulfilment of the identified tasks and increase the effectiveness of combating the aforementioned threats the following tools and communication and information systems are being implemented. 1) a system allowing the operational control of network traffic, 2) agent systems for the surveillance of information systems, profiled to track illegal activities and intended to support the course of Internet monitoring; 3) the system for searching, indexing and analysis of illegal content on the Internet; 4) a system for exchanging information about offences committed using the Internet[12].

Current activities performed by police officers dealing with computer crime are mainly focused on the elimination of information theft, computer system hacking, illegal content dissemination, illegally obtaining goods based on generated credit or debit card numbers, stealing electronic call and data billing units, illegal production and distribution of works protected by copyright, and SIM card cloning. Polish cyber-police cooperates with international institutions, which facilitates the exchange of information and international

[11] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016, http://bip.msw.gov.pl/bip/programy/ 19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.
[12] Ibidem.

training for young police officers. Thanks to the collaboration with Interpol, Europol, and the Central Bureau of Investigation, the participation of foreign actors in criminal activities does not pose such problems as previously (Wojciechowska-Filipek, Ciekanowski, 2016: 243).

The next important institution in the protection of cyberspace is the National Cybersecurity Centre ("NC Cyber") established on 5 July 2016. It is an early warning centre which, working on a 24/7/365 basis, manages and monitors the procedure of issuing information about network threats. The Centre also deals with notifications of harmful and illegal content (Dyżurnet.pl[13]). The NC Cyber is developing a national protection plan, in cooperation with the administration, business, and scientific communities. The NC Cyber operates within the structures of the NASK, and consists of four divisions – Operations, Research & Development, Analysis, and Training. Within the Operations Division there is the National CERT team, i.e. a group which, among other things, responds to network security incidents, constantly monitors threats in cyberspace, and anticipates upcoming trends and threats. Thanks to the cooperation with such entities as banks, mobile-phone operators, power-line managers, energy distributors, etc., CERT specialists have direct access to the IT infrastructure of the whole country. If a cyber-attack from outside is detected, it is intended to make it easier to defend against it at the Polish IT border. As part of their cooperation with the NC Cyber, the individual institutions have deployed their specialists, who monitor the situation in cyberspace 24 hours a day, to its Headquarters. Their presence is designed to facilitate rapid response in the event of an adverse situation[14].

The NC Cyber acts as a security operation centre (SOC) in the field of cybersecurity, carries out audits of companies and public administration authorities which encompass critical infrastructure. It also issues guidelines and recommendations. The NCC NASK is the place where information on threats from the various actors involved in the project is collected as part of the National Cyberspace Protection System. The NASK's NC Cyber specialists conduct analyses and make recommendations on the basis of this information. The NC Cyber develops contingency plans, organises training and drills for persons responsible for the security of the state administration, and stipulates minimum security requirements for institutions. The NC Cyber will prepare incident-reporting schemes, which will include critical-infrastructure managers, banks, and other business sectors[15]. The Centre plays a key role in the process of implementing the EU NIS Directive in Poland.

[13] Dyżurnet.pl is the point of contact for receiving reports of illegal content on the Internet (in practice, most of it relates to paedophilia and child pornography, but there are also those which involve racial, ethnic and religious hatred).
[14] https://mc.gov.pl/aktualnosci/ncc-na-strazy-cyberbezpieczenstwa.
[15] http://www.cyberdefence24.pl/398863,na-bazie-cert-polska-rusza-narodowe-centrum-cyberbezpieczenstwa.

In conclusion, in recent years we have seen a spike in interest in cybersecurity, resulting in an increasing number of individuals and organisations emerging to deal with this problem. However, in order to carry out public tasks in this area more effectively, it is necessary for administrative, military, and civil fields to cooperate and exchange information. It is also essential in these fields to build structures and systems protecting the information which forms the basis of their operations.

2 Information security policy, information security management system in administration

Currently, when the activities of organisation and administration are mainly based on information, and the digitalisation of operations is a standard procedure, one of the most pressing issues for the administration in safeguarding security is to develop an information security policy, and create an information security management system. The administration will not be able to create a secure cyberspace for the functioning of the state and society if it does not have security mechanisms in place within its organisational structure.

Information security policy is a documented set of rules, practices, and procedures, in which a given administration organisational unit defines the way it protects its information system assets and data processing. It is a document which indicates the management's involvement in information security, and defines the influence of information security on the implementation of, and support for, the administration's mission and vision (Wojciechowska-Filipek, Ciekanowski, 2016: 156).

The security policy is developed in several stages, including 1) needs analysis – identifying threats, estimating potential damage, inventorying the information system, defining requirements, analysing possible solutions, defining an optimal investment method; 2) definition of security policy – defining targets, marking out interdependencies, defining information flow, publishing security rules, planning training sessions, and methods for the monitoring and control of the application of security policy; 3) implementation of the security policy – publishing the security policy, appointment of teams, assigning tasks, verifying the knowledge of security policy; practical training, providing information on important events and changes; 4) controlling, security monitoring – confronting reality with the planned policy, security audit, review of security-related events, monitoring system activity, collecting and analysing information, checking the level of knowledge of security principles among the staff (Nowicki, Unold, 2002: 174-175).

In fact, an information security policy explains the need for information security, its concept in relation to all the users of the organisation’s information resources, and reflects the preparedness for acting in a controlled and safe way.

An information security policy is composed of: 1) the need for, and scope of, information security – an introduction, stressing the organisation's dependence on information, and thus on information security. This introductory declaration provides the background for the reasons why such policy is indispensable for the organisation; 2) information security objectives – should be described briefly, to inform the readers about the specific objective of information security management in the organisation. The objectives should be clearly linked with the organisation's general strategy and business goals; 3) the definition of information security – information security policy is usually addressed to various recipients, for whom information security might be a new notion. Therefore, it is essential to briefly define information security in a clear way in order to ensure a uniform understanding of the term across the organisation, 4) management involvement – a declaration of management involvement is the most important element of information security policy. Without that, no measures taken by the staff attempting to remedy flaws in information security will be effective or treated seriously across the organisation; 5) approval of the Information Security Policy – signature of a senior management member, 6) objectives of information security policy – this sections should describe the main objectives of the security policy itself; 7) information security rules – this part describes the general principles related to information security in the organisation. It explains to the users what the proper conduct in the organisation should be like. Some of the principles would be closely related to the organisational culture or regulatory requirements applicable to the sector in which the organisation concerned operates. Other rules will apply to all organisations, such as protection against viruses or user education; 8) roles and responsibilities – it is one of the most important elements of the information security policy. This parts provides the readers with details of the expectations in the scope of information security in the organisation. The tasks and obligations should entail all aspects of information security and individual obligations of all the parties using the organisation's information resources; 9) information security breach – statement on an information security breach – guarantees that the disciplinary proceedings will be instituted against a user who has failed to observe the security policy; 10) monitoring and verification – refers to the need of frequent monitoring and the effectiveness of inspecting information security within the organisation (Hone, Eloff, 2002; 402-404).

Generally speaking, a policy is a set of cohesive, precise rules and procedures compliant with the applicable laws, under which a given organisation – administration builds, manages and provides access to information resources (Wojciechowska-Filipek, Ciekanowski, 2016: 157).

The most important benefits of a well-developed security policy include: 1) the distribution of the responsibility for the development of the system across separate groups of people, so that no one has full power within the system; 2) establishment of organisational structures responsible for information security management; 3) control accompanying the issue of cards and codes is not left to programmers who have access to account data; 4) introduction of a distinction into open and protected information; 5) division of operational functions between several staff members; 6) effective

programming of information security principles among the management and employees of the organisation; 7) the documentation of changes to the system allows periodic system reviews; 8) the supervision over software modification and system testing, 9) regular user training in respect of information security; 10) backup copies stored in other premises than the room where the server is located, 11) system monitoring and detection of anomalies (Matuszczyk, Matuszczyk, 2006: 99-101).

It is clear that information security is a key issue in today's administration. Therefore, information security management systems comprise part of an organisation's management system. It is based on an approach resulting from business risk management, and refers to establishing, monitoring, implementing, maintaining, and improving information security (Kreft, 2010: 4).

The objectives of information security include: 1) providing optimum information protection cost-wise; 2) defining the risks which can be avoided, and how such risk can be avoided, by applying both organisational and technical solutions in the scope of storing, processing and transferring information, 3) reducing risk to an acceptable level (Liderman, 2002: 78).

At every institution covered by the National Cybersecurity System Act, a given unit's head must establish a cybersecurity management system based on the existing standards and best practices. These should define, among other things, the roles of the administrators and security inspectors of information processed in open communication and information systems and networks. The information-security management system will thus become an integral part of the institution's security policy[16]. Public entities modify, develop, and implement, as appropriate, security policies for the communication and information systems used by these entities to perform public tasks[17]. In drafting their security policies, public entities take into account the responsibilities stipulated by the Act on the Computerisation of the Business Entities Pursuing Public Tasks, regarding the minimum information security requirements for communication and information systems[18]. A public entity should also take into account the provisions of the Polish Standards in the field of information security, in particular the group of standards in the PN ISO/IEC 27000 series, along with other related standards[19]. Coordinating the

[16] The Cybersecurity Strategy of the Republic of Poland for 2017-2022 https://mc.gov.pl/aktualnosci/ strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.

[17] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

[18] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/ polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.

[19] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

information security policy of organisational units will ensure a common minimum level of security. When considering cybersecurity, all institutions are obligated to establish, implement, monitor, operate, review, maintain, and improve their Information Security Management Systems ("the ISMS")[20]. The Minister competent for computerisation, in accord with the Ministry of National Defence (the MON), the Internal Security Agency (the ISA), and the Military Counterintelligence Service (the MCS), with the intention of guaranteeing a uniform information security policy for organisational units, has the power to draw up guidelines for information security management systems[21].

When the appropriate regulations are implemented at the statutory level, the following will be ordered. 1) Reporting on information security incidents to a designated governmental centre; 2) Drawing up Disaster Recovery Plans (DRPs) and Business Continuity Plans (BCPs), after the occurrence of an incident, including national standards or, in the absence thereof, international standards, acceptable principles not included in official standards, or widely recognised good practices; 3) Managing information security and the introduction of safeguards, including national standards or, in the absence thereof, international standards, acceptable principles not included in official standards, or widely recognised good practices; 4) Operating within a network of information about hazards[22].

The ISMS (Information Security Management System) is understood (as defined in the ISO/IEC 27000 series of standards) as a part of the management system based on the concept of business risk management, responsible for establishing, monitoring, implementing, operating, reviewing, maintaining, and improving information security[23], the management system itself being understood as a set of guidelines, policies, procedures, processes, and related resources (i.e. material resources – such as computers and machines; human resources – such as employees, with their skills and experience; and intangible resources – such as computer programs and organisational culture) aimed at ensuring that the organisation completes its tasks (Gillies, 2011: 367-376, Humphreys, 2007: 11-44). At least two elements in the normative definition should be stressed (Lisiak-Felicka, Szmit, 2016: 62): 1) the systemic approach, especially as the information security management system is composed not only of "paper" records (procedures, standards,

[20] The Cybersecurity Strategy of the Republic of Poland for 2017-2022 https://mc.gov.pl/aktualnosci/ strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.
[21] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/ polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.
[22] The Cybersecurity Strategy of the Republic of Poland for 2017-2022 https://mc.gov.pl/aktualnosci/ strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022.
[23] ISO/IEC 27000:2014 Information technology – Security techniques – Information security management systems – Overview and vocabulary. https://www.iso.org/standard/63411.html.

ordinances, etc.) but also of all the resources relating to information security; 2) basing information security on the business risk management concept"[24].

According to § 20 (1) of the Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework (KRI), the minimum requirements for public records and the exchange of information in electronic form, and the minimum requirements for communication and information systems (consolidated text, Polish Journal of Laws of 2016, item 113), "the KRI Regulation", the entity performing public tasks develops and establishes, implements and operates, monitors and reviews, and maintains and improves, an information security management system, ensuring the confidentiality, availability, and integrity of information, taking into account such attributes as authenticity, accountability, non-repudiation, and reliability. The requirements for the information security management system in the KRI Regulation are considered to be fulfilled if the system "has been developed on the basis of the Polish Standard PN-ISO/IEC 27001, and the establishment of safeguards, risk management, and auditing is carried out on the basis of Polish Standards related to this standard, including: 1) PN-ISO/IEC 17799168 – with regard to the establishment of safeguards; 2) PN-ISO/IEC 27005 – with regard to risk management; 3) PN-ISO/IEC 24762 – with regard to IT-disaster recovery within business continuity planning (Lisiak-Felicka, Szmit, 2016: 64).

As regards the information security management system, the most important standards are 1) PN-ISO/IEC 27001:2014–12 – Information technology – Security techniques – Information security management systems – Requirements: specifies the requirements for the establishment, implementation, maintenance, and continuous improvement of the information security management system with regard to its organisation. It also includes the requirements for estimating and handling information-security risks; 2) PN-ISO/IEC 27002:2014-12 – Information technology – Security techniques – Code of practice for information security controls contains recommendations for information security standards in organisations, and information security management practice, including the selection, implementation, and management of safeguards, taking into account the environment(s) in which information security risks are present in the organisation. Chapters 5 to 18 relate to the safeguards listed in Annex A of the 27001 standard (Lisiak-Felicka, Szmit, 2016: 64).

It should be noted that the new possibilities for the administration's operation, and, in particular, the virtualisation of its activities, also generate an ever-increasing risk of interference with information security. Risk management is the element of key importance in the process of protecting cyberspace. It determines and justifies measures undertaken to reduce the risk to an acceptable level. The first stage in risk management is the identification of all cases of hazards, and the identification of their sources and

[24] PN-ISO/IEC 31000:2012 – Risk management – Principles and guidelines http://pbsg.pl/polski-komitet-normalizacyjny-pbsg-polrisk-i-zakonczyly-z-sukcesem-prace-nad-opracowaniem-pierw/.

impacts. Each identified risk should then be evaluated and categorised, using the defined risk categories and parameters, and prioritised (Wojciechowska-Filipek, Ciekanowski, 2016: 160). This is very important in the context of taking potential preventive actions against key risk types, in line with the risk management and implementation strategy adopted in order to regularly monitor the status of each risk (Crapko, 2012: 215-266). The adopted action plan will direct most of the resources (technical and non-technical) against the most likely risks. Information-security risk assessment should be performed repeatedly during business operations.

Only in such an event will it bring multiple benefits for the organisation, including: 1) demonstrating whether an organisation must control information security; 2) ensuring that security measures are applied properly and efficiently, in line with appropriate information classification; 3) identifying and recommending corrective measures in the event of a "successful" cybersecurity incident (Broderick, 2001: 15).

It should be stressed that risk management is not intended to provide total protection, but to ensure a level of protection proportionate to the importance of the resources being protected. Risk management is a process which consists of both identifying hazards and assessing risks, by deciding which risks are to be avoided, and which ones to control, and how. An organisation, such as an administrative unit, can take action to avoid risks by refraining from high-risk operations, such as, for example, introducing 'top secret' information into the system. It can also transfer the risk to another entity with the use of a legal mechanism, e.g. to insure itself against a given risk. The administration can also consciously control risks in two ways (Wojciechowska-Filipek, Ciekanowski, 2016: 160).

One of these is to minimise risk by implementing business continuity plans to ensure that users have access to the most important organisational functions in an emergency situation. In the event of a crisis situation, organisations should apply data and information security procedures, for example, 1) have a backup archive at another location if possible; 2) data stored on hard drives should be copied to two independent external media, and regularly returned and stored in a safe place; 3) if you have important paper documents, you should photocopy or scan them, and store them in a safe place, such as a safety deposit box; 4) prepare precise instructions in the event of an emergency shut-down of equipment, especially computer hardware" (Murdoch, 2003:22).

The second way to control risk is prevention by using safeguards.

Ways of reducing risk: 1) risk avoidance; 2) risk control; 3) prevention through safeguards (non-technical safeguards, technical safeguards); 4) minimising by implementing business continuity plans; 5) risk transfer (Murdoch, 2003: 22).

On the last day of January each year, with the intention of achieving an acceptable level of security, all government administration units referred to in the Cyberspace Protection

Policy of the Republic of Poland[25] ("the Policy") provide the Minister competent for computerisation with a report summarising the results of risk assessment (according to the model developed by the Minister competent for computerisation). The report should include general data relating to hazards, risks, and vulnerabilities identified in each of the sectors in which the institution operates and for which it is responsible. The report also presents information on methods for dealing with risk. The Minister competent for computerisation, in cooperation with the institutions involved, formulates a uniform methodology for conducting risk analyses. This methodology is obligatory for government administration institutions. The Governmental Computer Security Incident Response Team CERT.GOV.PL submits to the Minister competent for computerisation, with a view to achieving a unified approach, catalogues covering vulnerabilities which undermine cybersecurity, and the specification of possible threats[26].

Plenipotentiaries for Cybersecurity *("the PfC")* have been appointed within government-administration units.

The PfC performs the following tasks regarding cybersecurity: 1) Drawing up and initiating procedures for responding to computer incidents, which will function within the organisation; 2) Developing contingency plans and their testing; 3) Performing tasks resulting from the provisions of legal acts dedicated to ensuring security in cyberspace; 4) Identifying and conducting periodic risk analyses; 5) Preparing procedures to ensure the notification of the appropriate CERTs[27].

The position of a Cybersecurity Representative within the structure of the organisational unit is not indicated by the Policy; however, this role should be performed by a person responsible for the implementation of the ICT security process[28].

In summary, an information security policy is a set of precise and consistent procedures and rules, according to which a given public-administration institution manages, builds, and makes available information and communication resources and systems. It determines which resources are to be protected and the methods applied to this end. The ISMS, on the other hand, is a continuous process which must be constantly improved and adapted to changing circumstances. Each stage is divided into activities which involve security policy, as well as risk and resource management. Combining all activities into a continuous process of secure information management facilitates the secure functioning in the new digital reality.

[25] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.
[26] Ibidem, p. 160.
[27] Ibidem, p. 161.
[28] Ibidem, p. 162.

The information security policy places significant emphasis on the protection of information. As part of such activities, a special position is held by the protection of classified information, being information whose unauthorised disclosure could cause serious damage to the Republic of Poland, or would be unfavourable from the perspective of the state's interests, including during the development of such information, and notwithstanding the form and method of expression (Karpiuk, 2015:137-147; Bożek, Czuryk, Karpiuk, Kostrubiec, 2014: 66-75; Karpiuk, 2018: 85-99; Karpiuk, Chałubińska-Jentkiewicz, 2015: 151-173; Chałubińska-Jentkiewicz, Karpiuk, 2015a: 33-40)

3 Threats to information and information systems

In the context of information systems and their vulnerabilities, security is mainly focused on the technical aspects, such as data encryption and access control methods. It should be stressed, however, that the systems were developed for the benefit of people and are operated by them (Wojciechowska-Filipek, Ciechanowski, 2016: 138). This adds additional dimensions to the subject matter, including the legal, sociological, psychological and cultural aspects (Białas, 2006: 28). As a result, security threats have an interdisciplinary character and comprise: 1) general threats: a) disclosure of information to unauthorised persons, b) design of a defective information infrastructure, c) theft of resources, d) improper use of resources, e) eavesdropping; 2) environmental and criminal threats: a) natural disasters – water, fire, b) criminal activity – hacking, extortion, assaults, etc., c) terrorism; 3) threats resulting from psychological aspects: a) activities of computer intruders, b) dishonest employees, c) human error and mistakes, d) intentional acts committed by dishonest employees, 4) threats resulting from unfair competition; a) credit information agencies, b) opinions of other entities within the sector, c) document verification (Wojtaszek, Materska-Sosnowska, 2009: 196-197).

Threats can be classified on the basis of various criteria, mostly in terms of the location of the threat source or randomness.

The most frequent classifications in the literature on the subject include a division into 1) accidental and intentional threats – accidental threats include: hardware break-down, user omission and errors, and software errors. Intentional threats are deliberate actions of system users; 2) passive and active threats – passive threats occur in the moment of unauthorised disclosure of information, but without compromising or affecting an information system. These include eavesdropping, network traffic analysis and compromising emanation. Active threats are those threats where information is modified with the intention of corrupting or destroying the data or the network itself; 3) internal and external threats – internal threats are caused by authorised system or network users The main causes of such threats include: a) lack of business continuity plans, b) excessive privileges of employees, c) lack of security policy, d) lack of incident documentation, e) failure to respond to irregularities or responding too late (Pilawski, 2000: 4); 4) hardware and software threats – hardware threats comprise irregularities in the operation of

computer hardware. Software threats are related to errors occurring in software functions (Wawrzyniak, 2002: 40).

Depending on the impact of potential threats on the functioning of an organisation, threats can also be classified as 1) operational threats – affecting the day-to-day financial operation and capital of a company; 2) strategic threats – affecting the long-term goals of a company; 3) compliance threats – affecting compliance with the legal regulations in force (Liderman, 2002: 44).

Taking into account the place of origin of a given threat, attacks can be classified as 1) remote attacks – where an Internet service is the target or where the victim is in another network; 2) local attacks – where the perpetrator has physical access to the victim's computer; 3) internal – where the attacker and the victim are located in the same network (Pilawski, 2000: 4).

In 2013, as part of risk assessment in public administration agencies, the Ministry of Administration and Digital Affairs adopted the following classification of cyberspace threats: 1) threats directed against communication and information infrastructure, including: a) interception of a communication and information system (downloading resources by installing malware or using botnets, or vulnerabilities in devices of specified manufacturers (sometimes left intentionally), b) deletion of data (e.g. changing information on a website by gaining access to the network server which has vulnerabilities, which is most often related to the failure to update content management software), c) disruption of operation (e.g. denial of service attacks, focused on blocking the availability of specified electronic services for an extended period or the use of ransomware; d) IT break-downs (natural disasters, technical malfunctions or human error); e) insufficient skills (some staff members have insufficient awareness and knowledge of cyberthreats, and are not qualified to counteract such threats independently); 2) threats directed against information, including a) the provision of false information (applied in financial fraud, consisting in unauthorised alteration of information – e.g. change of bank account numbers), b) information theft with the intention to publish or sell it (may consist in, e.g., targeted espionage with the use of APT techniques, information theft using botnets or publication of information about vulnerabilities by Internet activists)[29].

According to W. Gogołek, threats in cyberspace can be divided into seven categories: 1) protocol failures – using vulnerabilities in the set of rules controlling data exchange between two or multiples independent devices or processes; 2) stealing passwords – methods consisting in obtaining network access passwords, 3) information leakage – the attacker obtains information available only to the administrator; 4) social engineering – using the incompetence of persons who have access to a communication and information

[29] Raport o stanie bezpieczeństwa w Polsce *[Report on the state of security in Poland]*, MSW 2014. https://isp.policja.pl/download/12/7854/ RAPORT2014OSTATECZNY.pdf.

system; 5) authentication failures – destruction of an authentication mechanism; 6) bugs and backdoors – use of illegal software or use of a system without special authorisation; denial of service – where the users are unable to access the system (Gogołek, 2007: 321).

The security of information systems, which is increasingly important in our societies, covers numerous aspects, and the fight against cybercrime belongs to its core elements (Chałubińska-Jentkiewicz, Karpiuk, 2015b: 12).

The notion of cybercrime, and the terms "computer crime", "computer-related crime" or "high-tech crime" which are often used interchangeably[30], understood as criminal acts committed using computers connected to the Internet, or via the Internet, affecting, i.a. the security of information technologies, have found their place both in the views of legal commentators, and of experts dealing with ICT security (Czyżak, 2009).

From the historical perspective, one of the first definitions of computer crime was included in a comprehensive description of computer crimes of 1979, whose lead author was Donn B. Parker – Criminal Justice Resource Manual on Computer Crime (Kosiński, 2015: 35). Computer-related crimes, defined in the Manual as a broader category, are any violations of criminal law that involve a knowledge of computer technology for their prosecution (Kosiński, 2015: 35).

In a study on the international legal aspects of computer crime of 1983, computer crime was consistently defined as crime which "encompasses any illegal act for which knowledge of computer technology is essential for its perpetration" (Schiolberg, 1983).

In the 1996 edition of "*Kryminalistyka*" Prof. Brunon Hołyst cited Donn B. Parker's definition of computer crime, understood as acts in which victims suffered loss, damage or injury and in which data processing systems were used (Hołyst, 1996: 241).

In the Communication from the Commission of 2001, computer-related crime was described in its broadest sense as "as any crime that in some way or other involves the use of information technology"[31]. Moreover, the Communication makes a distinction between "computer specific crimes" and "traditional crimes performed with the aid of computer technology" (Kosiński, 2015: 45).

In the aforementioned Cybersecurity Strategy of the European Union, it was stated that cybercrime commonly refers to a broad range of different criminal activities where

[30] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions – Towards a general policy on the fight against cyber crime, 22 May 2007.
[31] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" of 26 January 2001.

computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware) (Kosiński, 2015: 45; Feret, 2020: 89).

The notion of cybercrime was defined in Poland in the Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016, and repeated in the Cyberspace Protection Policy of the Republic of Poland of 2013. In those documents, cybercrime was defined as an offence committed in cyberspace[32]. The documents also provide definitions of cyberterrorism, understood as an offence of a terrorist nature committed in cyberspace (Kosiński, 2015: 46).

According to K. Chałubińska-Jentkiewicz, and M. Karpiuk, cybercrime includes offences committed with the use of electronic communications networks and information systems, or directed against such systems. In practice, the notion of cybercrime is used in relation to three types of offences. The first type includes traditional forms of crime, such as fraud or forgery, but in the context of cybercrime these prohibited acts refer specifically to offences committed over electronic communication networks and information systems. The second type involves the publication of illegal content over electronic media (e.g. materials related to the sexual exploitation of children or incitement to racial hatred). The third type comprises crimes unique to electronic communications networks, e.g. attacks against information systems, denial of service or hacking (Chałubińska-Jentkiewicz, Karpiuk, 2015b: 12).

Cybercrime includes the following categories of offences: 1) fraud committed via the Internet; 2) paedophilia and child pornography – the Internet allows paedophiles not only to obtain and disseminate child-pornography materials, but also to establish contacts with minor children to arrange a meeting and to exploit them sexually; 3) trade in licensed products without proper documentation, or trafficking illegal goods, i.a., narcotic drugs, or precursors used in their production, explosives and chemical reagents used for their production; protected animal species); 4) crime with the use of electronic payment instruments, including phishing, which consists in obtaining sensitive data via the Internet (passwords, ID, logins, etc.), allowing the illegal performance of financial operations by electronic means (the Internet) on bank accounts, without the knowledge and authorisation of their rightful owners; 5) illegal trade in national heritage goods and trade in objects obtained by way of criminal activities, 6) illegal trade in goods subject to excise tax, including tobacco products; 7) offences resulting in losses incurred by owners of intellectual property rights (in particular by way of illegal distribution of music, films, computer games or software); 8) human trafficking and trafficking of human organs; 9) unauthorised access to information (hacking), blocking access to information, computer

[32] Page 6 of the Programme and the Policy, Point 1.1. Definitions.

sniffing, malware, breach of computer safeguards, etc.; 10) extortion or unlawful threats by organised criminal groups; 11) illegal gambling via the Internet[33].

The European Commission considers the following offences as cybercrime: 1) manipulating invoices or company accounts, computer forgery, fraudulent auctions or illegal use of credit cards, attacks against human life, child abuse, manipulating hospital systems or air traffic control, 2) content-related crime, including child pornography, child abuse, proposals to commit crime, providing instruction for criminal conduct, disseminating false information, and internet gambling and on-line lobbying, 3) crimes against the confidentiality, integrity and availability of data, concerning illegal access to systems – hacking, computer espionage, eavesdropping, providing false identities, sabotage and computer extortion; 4) crimes related to the breach of copyright and related rights, such as the unauthorised distribution and copying of computer programs, unauthorised use of databases" (Szubrycht 2005: 174).

According to the Cyberspace Protection Policy of the Republic of Poland, a cybercrime is every act which meets the two following criteria jointly: 1) it is a prohibited act within the meaning of any legal provisions; 2) it is committed in cyberspace, understood not as a geographic category, but a novel, logical domain of human activity, built on the broadly understood ICT infrastructure, but not treated as equivalent to the infrastructure (cyberspace as a virtual environment, separated from the physical substratum)[34].

As regards Polish studies, the notion of cybercrime was also used by A. Adamski, who grouped cybercrime into the following categories: 1) crimes related to the use of computers (e.g. computer-related forgery, computer-related fraud); 2) crime against conditional access to information services (e.g. unauthorised access to a subscription television service); 3) crimes against the confidentiality, integrity and accessibility of computer data and systems (e.g. data transmission eavesdropping, unauthorised access to a system of disruption of system operation), 4) crimes related to the distribution or transfer of specified types of information (e.g. child pornography, promoting racist contents, or even sending unwanted commercial information, so called spam) (Adamski, 2005: 51-52).

In the Council of Europe Convention on Cybercrime, (Convention on Cybercrime made in Budapest on 23 November 2001 – Polish Journal of Laws of 2015, item 728), hereinafter the Council of Europe Convention, cybercrime was defined in four categories, including 1) content-related offences, e.g. sexual abuse and mobbing via the Internet, child pornography, proposals to commit crime, providing instructions for criminal conduct, Internet gambling, disseminating false information; 2) Computer-related

[33] Raport o stanie bezpieczeństwa w Polsce *[Report on the State of Security in Poland]*, MSW 2014. https://isp.policja.pl/download/12/7854/ RAPORT2014OSTATECZNY.pdf (May 24, 2017).
[34] www.cert.gov.pl/download/.../PolitykaOchronyCyberprzestrzeniRP148x210wersja_pl.pdf (May 24, 2017).

offences: from the traditional crimes (e.g. fraudulent auctions, manipulating invoices, company accounts, illegal use of credit cards), through computer-related forgery, to attacks on human life (e.g. manipulating hospital systems, air traffic control systems, or healthcare systems); 3) offences against the confidentiality, integrity and availability of computer data and systems, e.g. deceiving authorised users, illegal access to systems by hacking, eavesdropping, sabotage, computer-related extortion (e.g. viruses, DDoS attacks, spam), and computer espionage (Trojans and other techniques); 4) offences related to infringements of copyright and related rights, e.g. unauthorised use of databases, distribution and copying of computer programs (Kowalewski, Kowalewski, 2014; Radoniewicz, 2016: 162-194).

Public administration systems are most susceptible to cyber-attacks, as they are seen as equivalent to state authorities (Burdzial, Cieślak, Rodzewicz, 2011). Internet-related threats may take various forms. The attacks used in such type of activities usually include: 1) DDoS, a variant of DoS, has the same function as DoS, but multiple computers are used to carry out such attack; 2) DoS – is aimed at blocking the operations of a computer network and the use of its services by overloading the targeted machine (server), and a single computer is used to carry out the attacks; 3) SYN flood – its objective is to block a network server by exploiting the TCP protocol, resulting in the overload of a computer network; 4) Fork bomb – leading to a total crash of a system and making server connection impossible (Kowalewski, Kowalewski, 2014:; Radoniewicz, 2016: 108-112).

Issues related to information security are of particular importance in the case of wireless networks, which results from the fact that the access to such networks is not limited in physical terms, because radio waves are the transmission medium in this case. Wireless networks can be subjected to three types of threats, i.e. interception of information, distortion of information, and blocking information transmission[35]. There are several types of attacks against wireless networks: 1) "War Driving" – searching for unsecured networks; 2) "Rogue Access Point" – an "undercover base station", an additional access point allowing access to data transmitted via the networks, 3) "Man-in-the-Middle" – also referred to as total eavesdropping, aimed at intercepting all network communications and collecting important and confidential information, 4) Sniffers – allow access to encrypted information and its decryption with the use of a WEP key[36].

APT (advanced persistent threat) attacks are becoming increasingly difficult to counteract. They involve various types of tools (software, social engineering, etc.) Preparations for an APT attack can take weeks or months. They are usually carried out by organised groups having a substantial budget, and in some instances they consist in the infiltration of a specific target – an institution or a company, which further allows the

[35] http://www.itfocus.pl//porady-ekspertow/wi-fi/zagrozenia-zwiazane-technologiami-bezprzewodowymi-wi-fi.
[36] Ibidem.

perpetrators to carry out a precise attack, aimed at damaging or destroying a computer system and stealing sensitive data (Grzelak, Liedel, 2014).

Cyberspace is the place of operation of individual perpetrators, organised criminal groups, extremist circles and terrorist organisations, which focus on cyberterrorism activities.

According to an American expert on cybersecurity, D.E. Denning, cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. To qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear (Kisielnicki, 2008: 352). In the current digital reality, cyberterrorism is unpredictable, i.a., due to the global reach of the Internet. It is an instrument of coercion used by organised terrorist groups to interfere in the operation of critical infrastructures of a given state, including the national transport, power supply, communication, water supply and financial systems (Bógdoł-Brzezińska, Gawrycki, 2003: 49).

Two aspects of an information threat resulting from cyberterrorism can be listed, and these are: 1) information technology as a tool; 2) and information technology as a target (Szubrycht, 2005: 183).

If information technology is a target, terrorist acts are aimed not only at computer sabotage, but also at physical sabotage, as in the case of the latter, terrorists use the network for the purpose of theft, manipulation or extortion (Szubrycht, 2005: 183). Terrorist groups, exploiting the opportunities which the Internet offers, send instructions, maps, and orders to coordinate terrorist actions. The medium is also used as a tool for conducting politically motivated activities and acquiring new supporters and funds for further operations. The Internet is also a place where members of terrorist organisations search for information necessary to carry out conventional terrorist attacks[37].

P. Sienkiewicz identified six key reasons why terrorists exploit the Internet to reach their specific objectives: 1) the disappearance of boundaries (states lose some of their sovereignty) – boundaries blur between the private and the public, the military and the commercial areas, etc., and the consequence of removing barriers is the probability that a given state will not be aware that it is under attack (blurred boundaries between war and peace); 2) low costs of such operations, especially when compared with the costs of regular military operations; 3) the possibility to perform immediate and unpredictable actions – the victims are left totally unaware and unprepared for defence; 4) instead of attacking innocent people, the system of an enemy state can be paralysed; 5) total

[37] http://academicon.pl/blogi_naukowe/bezpieczeństwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie-spoleczenstwa-informacyjnego.

anonymity – allows the possibility to manipulate information, and to hinder defence against the attacks and coalition-building; 7) improved effectiveness of propaganda activities and recognition among the general public (Bógdoł-Brzezińska, Gawrycki, 2003: 50).

In conclusion, the growing dependence of all kinds of activities on information, and transferring even a part of the activities to the Internet, generates numerous threats both within and outside the administration. The lack of proper safeguards, threat detections systems or plans of response to a situation of threat might lead to the theft or destruction of information, damage to an information system, or both, and lead to serious consequences for state institutions and citizens.

The specific nature of cybercrime is the continued evolution and changeability of not only the tools applied but also the methods and patterns cybercriminals use. The cross-border nature of cybercrime allows them to commit offences from nearly any place in the world.

The greatest significance in the sphere of improving the security of information and information systems and combating cybercrime can be attributed to the development of ICT security, education of all users keeping pace with technology advancements, up-to-date legislation taking into account such technology advancements, and international cooperation between law enforcement authorities and their collaboration with the IT sector and academic circles. Creating conditions for the development of security in cyberspace will facilitate the protection of the emerging information society.

4 The aspects of building security in cyberspace

The current reality related to the improvement of cybersecurity in the Republic of Poland, requires international cooperation for the protection of cyberspace. The cooperation should be mainly based on such organisations as NATO, the UN and the EU. The development of a uniform safeguard system will guarantee a high level of protection in all collaborating countries.

In order to set the direction of the development of the cybersecurity system, and to identify the strengths and weaknesses of its operation, the Supreme Audit Office performed audits covering this area. Substantive reports were prepared, outlining errors and omissions and providing guidelines and recommendations to remedy the current situation.

The documents prepared over the years became a good basis for implementing the vision and responding to challenges faced by the Polish cybersecurity system. Thanks to substantive indications, Poland has an opportunity to become resilient to attacks and threats resulting from the presence in cyberspace.

The development and strengthening of international-level cooperation is an essential aspect of cyberspace protection. Participation in undertakings of organisations dealing with cybersecurity allows the monitoring of technical solutions adopted in other friendly states. It facilitates the creation of a uniform safeguard system, which is able to provide a high level of security in all countries associated in a given organisation. This can contribute to an efficient information exchange between individual teams, which created conditions for a rapid response to new threats generated on the Internet (Żukrowska, Grącik, 2006: 187).

The issue of ICT security[38] in Poland involves organisational, legal, technical and international spheres. It requires intense activity on the part of institutions responsible for security on the Internet, and authorities, both at the domestic and international level. In the event of a potential cyberterrorist attack, the safeguards of Polish ICT network structures are subject to ongoing improvement (Żukrowska, Grącik, 2006: 187). "The Government of the Republic of Poland, acting through its state institutions, government authorities, representatives, and by way of collaboration with non-governmental organisations, declares that it will take efforts to increase the security of Polish and international cyberspace"[39].

Polish cybersecurity incident response organisations belong to, or collaborate with, international organisations whose aim is to counteract threats in cyberspace. The organisations which exercise supervision over cyberspace include 1) the European Union Agency for Cybersecurity(ENISA), running activities within the structures of EU Member States, 2) NATO Cyber Defence Management Authority; 3) European Police Office (Europol); 4) the International Multilateral Partnership Against Cyber Threats (IMPACT); 5) Cooperative Cyber Defence Centre of Excellence (CCDCoE), operating as part of the North Atlantic Treaty Organization; 6) Forum of Incident Response and Security Teams (FIRST), an organisation bringing together CERTs (Computer Emergency Response Teams) worldwide; 7) and the European Union's Judicial Cooperation Unit (Eurojust)"[40].

[38] ICT security refers to the security of electronic data, computer systems and data transmission in communication and information networks (security of devices and transmission media) Lipiński Z. (2003) Bezpieczeństwo teleinformatyczne – Wstęp. Wykład 1 *[ICT Security – Introduction, Lecture 1]* (Opole: Faculty of Mathematics, Physics and Computer Science at the University of Opole), pp. 1-2.

[39] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.

[40] M. Stempień, Ochrona cyberprzestrzeni Rzeczpospolitej Polskiej a współpraca państw członkowskich Unii Europejskiej *[The Protection of cyberspace of the Republic of Poland and the cooperation between European Union Member States]* http://docplayer.pl/15658274-Ochrona-cyberprzestrzeni-rzeczpospolitej-polskiej-a-wspolpraca-panstw-czlonkowskich-unii-europejskiej-marta-stempien-8.html.

Poland, as a member of the North Atlantic Treaty Organization, not only participates in implementing the cyber defence policy, but also belongs to the NATO Cyber Defence Centre.

Three main tasks were identified as part of NATO's defence policy, and these are: 1) advisory and coordination activities regarding the issue of defence against cyber-attacks – these activities are the responsibility of a special unit of the Cyber Defence Management Authority (CDMA) supervised by the Cyber Defence Management Board. CDMA brings together the representatives of political and academic circles of NATO allies; 2) the support for NATO allies – such activities are undertaken by a special unit called Rapid Reinforcement Teams (RRTs) RRTs are sent to member states which are in an immediate need of assistance in the fight against cyberterrorist attacks. The group is a prototype for a cyber-army; 3) training and research – a research unit operating as part of NATO is the Cooperative Cyber Defence Centre of Excellence (CCDCOE) based in Tallinn, Estonia (Świątkowska, Bunsch, 2011).

As part of the Polish Cyberspace Protection Policy, the Head of the ISA acts as the National Focal Point. As regards the government sphere, the structures responsible for the coordination of response to incidents in computer systems and networks include 1) a military computer security incident response team at the Ministry of National Defence, in relation to computer systems and networks supervised by the Ministry of National Defence; 2) a government computer security incident response team, in relation to the cyberspace of the Republic of Poland[41].

The Head of the ISA and the Minister of National Defence, in collaboration with the Minister of the Interior and Administration, are direct CDMA partners.

NATO assigns particular importance to combating cyberterrorism, and to the protection and functioning of cyberspace. The following initiatives can serve as perfect examples here: 1) a decision made by NATO in January 2008 in Brussels under which the NATO Policy on Cyber defence was adopted, and the Memorandum on the Concept for Cooperative Cyber Defense Centre of Excellence was adopted in May 2008, as a result of a cyber-attack against Estonia; 2) a decision made by NATO in Prague in November 2002 on initiating the Cyber Defence Program and the NATO Computer Incident Response Capability, as a result of cyber-attacks against NATO systems during the Balkan War; 3) during the Summit in Lisbon in 2010, NATO Allies adopted a new strategic concept[42], pointing to cyber-attacks as one of the most significant threats to the Allies of the North Atlantic Treaty Organization (Kowalewski, Kowalewski, 2014).

[41] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.
[42] The 22nd NATO Summit in Lisbon was held between 19 and 20 November 2010 in Portugal. Summit meetings of Heads of State and Government Lisbon, Portugal-Topics (EN) nato.int.

In May 2008 in Brussels, the Chiefs of General Staff of Lithuania, Spain, Estonia, Latvia, Slovakia, Germany and Italy signed a Memorandum on the Concept for Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn. In November 2001, Poland and the United States joined the Centre. It brings together experts from numerous allied states, Germany, Slovakia, Italy and Estonia. Poland has full access to research results and expert opinions prepared by the CCDCOE. As part of the Treaty, the Computer Incident Response Capability team (NCIRC) has been operating since 2012, and it is responsible for training on the protection against cyber-attacks (Wojciechowska-Filipek & Ciekanowski 2016: 228).

In the context of cyberterrorism, in relation to an obligatory protection against cyber-attacks and intensive promotion of fundamental freedoms (Wojciechowska-Filipek, Ciekanowski 2016: 228), a non-profit organisation called the International Multilateral Partnership Against Cyber Threats (IMPACT) deserves special attention. The activities of IMPACT are aimed at analysing serious threats related to cyberspace and critical infrastructure. It brings together states from all continents of the world (Wojciechowska-Filipek, Ciekanowski 2016: 229). IMPACT operates in four areas: 1) conducting research on security, which result in expert opinions, and at the same time cooperating with over twenty Centres of Excellence and universities, 2) holding training, coordinating and providing locations for such training, and disseminating best practices at ministry level, 3) monitoring the status of cyberspace worldwide 24/7, IMPACT publishes information on its website and has a closed networks for specialist (like Facebook) available via the Global Response Center system; 4) running the Centre for Policy and International Cooperation (Wojciechowska-Filipek, Ciekanowski, 2016: 229).

ENISA is a European agency established by the European Union to ensure the security of information, and computer networks and systems. The Agency is an advisory centre, developing expert opinions, and in the future it is to become a support entity for governments in the sphere of ICT security[43].

ENISA was established under Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. ENISA defines main operational objectives, including: 1) facilitating cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues; 2) collecting appropriate information to analyse current and emerging risks and providing the results of the analysis to the Member States and the Commission; 3) enhancing cooperation between different actors operating in the field of network and information security; 4) tracking the development of standards for products and services on network and information security, and promoting risk assessment activities, interoperable risk management solutions; 5) providing the European Parliament, the Commission, European bodies or competent national bodies appointed by the Member

[43] https://www.enisa.europa.eu/.

States with advice, and where necessary, with assistance within its objectives; 6) assisting the Commission and the Member States in their dialogue with industry to address security-related problems in hardware and software; 7) contributing to awareness raising and the availability of timely, objective and comprehensive information on network and information security issues for all users; 8) expressing independently its own conclusions, guidelines and giving advice[44].

Since 1998 CERT Polska has been a member of FIRST (the global Forum of Incident Response and Security Teams), and in 2000 it joined TERENA TF-CSIRT, a task force bringing together response teams, and the Trusted Introducer Service operating within the structure of the task force. In 2005, the Abuse FORUM, a forum of Polish abuse teams, was established in 2005 on the initiative of CERT Polska, and in 2010, CERT Polska joined the Anti-Phishing Working Group, an association bringing together enterprises and institutions actively involved in combating cybercrime[45].

EUROPOL – The European Union Agency for Law Enforcement Cooperation. The objective of EUROPOL is to strengthen actions by competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime affecting two or more Member States. The Agency's mission is to contribute to law enforcement activities in the European Union in respect of combating this form of criminal activities (Wojciechowska-Filipek, Ciekanowski, 2016: 230).

EUROJUST – European Union Agency for Criminal Justice Cooperation – a European Union agency established as a Community body acting for security in Europe. EUROJUST is a prosecution-type entity. It coordinates the works of all Member States with a view to combating cross-border organised crime across the EU (Wojciechowska-Filipek, Ciekanowski 2016: 230).

Another international institution with which Poland cooperates as part of combating and protecting against cyberterrorism is the UN. As part of the UN, a special International Telecommunications Union ("ITU") was established, taking responsibility for the cybersecurity of member states. The ITU brings together not only countries but also enterprises (i.a. Telekomunikacja Polska S.A. and Polkomtel S.A.). In 2008, ITU initiated the implementation of the Global Cybersecurity Agenda ("GCA") whose main objective is to develop the concept for international cooperation in the defence of communication and information systems and networks.

The GCA strategy is based on several assumptions, including: 1) raising the awareness of states and communities – it is necessary to educate not only governments and specialists, but also the general public, and knowledge of the threats arising from the

[44] Ibidem.
[45] CERT Polska Report 2012. Analysis of ICT security incidents. https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2012.pdf.

network, and good practices must be disseminated; 2) providing uniform legislation – uniform definitions of computer crimes and the related sanctions. It is also necessary to provide training to the staff of state institutions; 3) instituting cooperation between organisational structures – in line with ITU assumptions, countries should introduce improved procedures for protecting against cyberterrorist attacks. To this end, collaboration between countries and institutions is indispensable; 4) standardising procedures and technical measures – international certificates applied in telecommunications should be standardised. Until 2013, two certificates applicable in numerous countries were introduced, X.509 public key certificate, and the H.264 coding standard; 5) international cooperation – collaboration between countries and individual organisations is essential. For example, ITU cooperates, i.a., with IMPACT, CDMA, CCDCOE and ENISA" (Świątkowska, Bunsch, 2011).

Currently, an effective protection of European critical ICT infrastructure against cybercrime is one of the European Union's strategic goals, and Poland also runs its operations within this framework[46]. The increase in the number of initiatives protecting European societies indicates the enhancement of EU's involvement in the sphere of cybersecurity. In order to ensure the security of information and communication structures, it is crucial to boost effective collaboration between competent agencies and ministries, international and private entities[47]. The development of effective mechanisms for information exchange between Member States will result in a more effective protection of cyberspace. A joint protection of cyberspace requires the unification of penal laws of Member States in relation to cybercrime. Practical and specific solutions allowing the Member States to measurably enhance cybersecurity are necessary to ensure the compatibility of Polish cybersecurity systems with the systems of international organisations and other Member States[48].

The adoption of the aforementioned Council of Europe Convention was a milestone in the implementation of the concept of international cooperation in the sphere of combating cybercrime. The Convention establishes the general principles relating to international co-operation in criminal matters for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence.

As regards to cooperation, the Council of Europe Convention regulates, i.a., 1) information transfer, 2) mutual assistance, 3) extradition, 4) 24/7 Network – Article 23 of the Council of Europe Convention.

---

[46] M. Stempień, http://docplayer.pl/15658274-Ochrona-cyberprzestrzeni-rzeczpospolitej-polskiej-a-wspolpraca-panstw-czlonkowskich-unii-europejskiej-marta-stempien-8.html.
[47] Cyberbezpieczeństwo Polski a Współpraca w Ramach Unii Europejskiej *[Cybersecurity in Poland and cooperation within the European Union]* http://www.academia.edu/17480644/Ochrona_cyberprzestrzeni_RP_a_wsp%82onkowskich_Unii_Europejskiej.
[48] Ibidem.

Under the provisions of the Council of Europe Convention, extradition is possible between two Parties for criminal offences, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty – Article 24 of the Council of Europe Convention. The Parties shall afford one another mutual assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail – Article 25 of the Council of Europe Convention. The Council of Europe Convention also imposes an obligation to provide information for the purpose of investigations. Several examples can be listed here, including: 1) institutions of one country forward to another Party information obtained within the framework of its own investigations when it might assist the receiving Party in initiating or carrying out investigations or proceedings; 2) a Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system; 3) the Parties are obliged to disclose the data stored on the servers of service providers – Articles 26-30 of the Council of Europe Convention.

The 24/7 Network is a point of contact available on a twenty-four hour, seven-days-a-week basis which should be designated by each Party. The points of contact serve other Parties who require assistance for the purpose of investigation, preservation of data, collection of evidence and technical advice – Article 35 of the Council of Europe Convention.

Another document which places emphasis on the development and strengthening of international cooperation is the aforementioned Cybersecurity Strategy of the European Union. The strategy aims to increase cooperation and transparency about security in ICT products. It calls for the establishment of a platform, bringing together relevant European public and private stakeholders, to identify good cybersecurity practices across the value chain and create the favourable market conditions for the development and adoption of secure ICT solutions[49].

It encourages increased international cooperation resulting in the smooth functioning of the underlying infrastructures that provide and facilitate communication services. This includes exchanging best practices, sharing information, early warning, joint incident management exercises, and so on[50].

[49] Cybersecurity Strategy of the European Union, p. 15.
[50] Ibidem, p. 19.

The table below demonstrates cooperation models in place as part of international cooperation.

Table 2: International cooperation model

Network and information security	Law enforcement	Defence	
• ENISA • CERT	• Europol • Eurojust	• European Defence Agency	EU
National CERTs	National cybercrime units	National security and defence authorities	STATE

Source: The Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace, Brussels 2013, p. 20

To address cybersecurity in a comprehensive fashion at the international level, activities should span across three key pillars: network and information security, law enforcement, and defence. It is essential to institute cooperation between organisations and state institutions[51] in each of the pillars, as shown in the model above.

The next important document on international cooperation, adopted by the European Parliament on 6 July 2016, is the NIS Directive: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union[52]. Under the provisions of the Directive, each Member States is bound by the obligation to achieve the expected effects. Member States may choose the forms and measures of performing the agreed provisions. Its objective is to contribute not only to implementing common patterns for the protection of services in Europe, but also to creating rules for the exchange of information on threats between individual Member States. Its objective is to support the implementation of common standards for the protection of services in Europe, but also to develop rules for the exchange of information on threats[53]. (Radoniewicz F. 2019:17-19).

The new EU laws impose certain obligations on the operators of essential services. The obligations include ensuring a proper level of security and notification of incidents. This refers to such sectors as energy, transport, healthcare, banking, drinking water supply, and digital services (search engines, cloud computing services)[54].

The new law also provides a possibility to establish strategic "cooperation groups", aimed at information exchange and support for Member States in their efforts towards ensuring

[51] Cybersecurity Strategy of the European Union, p. 7.
[52] 5581/1/16 REV 1. http://data.consilium.europa.eu/doc/document/ST-5581-2016-INIT/pl/pdf.
[53] https://www.cybsecurity.org/pl/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/.
[54] Ibidem.

security. Each EU Member State is obliged to adopt a national strategy on the security of network and information systems. Furthermore, Member States are obliged to designate Computer Security Incident Response Teams (CSIRT). The European Union Agency for Network and Information Security (ENISA) is intended to play a key role in the implementation of the Directive, in particular in the field of coordinating cooperation between individual States as part of the CSIRT network[55].

In general, it can be stated that cybersecurity may be achieved more effectively by way of international cooperation at the strategic and political level. The cooperation should be based on such organisations as NATO, the UN and the EU. As regards the European Union, measures as part of the cooperation must be based on a common approach to cybersecurity and on the compatibility of systems of individual Member States. Similarly to other Member States, Poland needs restrictive, and most of all effective, legal regulations which would adequately ensure the cybersecurity of state, EU and international structures and the private sector.

The Supreme Audit Office (NIK), exercising its powers, conducted two cybersecurity audits. The first audit, with its results published in the *Information on the Results of Audit "The Performance of Tasks in Respect of Polish Cyberspace Protection by State Authorities"*[56] on 23 June 2015, involved the inspection of tasks related to state ICT security. The auditors wanted to take a closer look at the cyberspace protection system of the Republic of Poland, whether such system was in place, whether there were entities operating within the system, whether their activities were coordinated and whether there was mutual support between the entities. The objective of the second audit was to check how individual systems of substantial importance to the functioning of the state were protected, including the e-farmer system operated by the Agricultural Social Insurance Fund, and the new electronic land and mortgage registry, or a system developed for the fulfilment of tasks by the Ministry of State Treasury[57].

The first audit covered the operations of the Internal Security Agency, the Ministry of Administration and Digital Affairs, the Ministry of the Interior, the Ministry of National Defence, the Office of Electronic Communications, the Research and Academic Computer Network, the Government Centre for Security and the National Police Headquarters (Lisiak-Felicka, Szmit, 2016: 156).

The Supreme Audit Office issued a negative assessment of the implementation of cyberspace security tasks by the aforementioned entities. The audit report listed a number

[55] Ibidem.
[56] The Supreme Audit Office. The implementation of tasks in the sphere of Polish cyberspace protection by state authorities: Information on Audit Results. https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf.
[57] G. Stech, NIK: Cena za cyberbezpieczeństwo będzie wysoka *[The price for cybersecurity will be high]*.http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.

of problems and shortcomings, and formulated an attempt to define the causes of the situation (Lisak-Felicka, Szmit, 2016: 156).
According to the key findings, there was no systemic approach to the issues of cybersecurity, measures were undertaken in a dispersed manner and were largely limited to a "temporary, small-scale response to ongoing incidents, and passive anticipation of solutions to be proposed by the European Union" (Lisiak-Felicka, Szmit, 2016: 157).

According to NIK, activities related to cybersecurity do not demonstrate preparedness or a coherent vision. Passive anticipation of the solutions to be proposed by the EU, and the lack of a single decision-making centre which would coordinate the operations of other public institutions have resulted in the inactivity of the state in this sphere[58]. It is possible to name such decision-making centres as the Internal Security Agency, the Ministry of National Defence or the Ministry of Digital Affairs. To some extent these entities compete against each other, often putting forward conflicting opinions on the direction of Polish cybersecurity[59].

No fundamental threats to the national information and communication infrastructure were identified, and no national cyberspace protection strategy was developed that would form the basis for measures taken with a view to increase ICT security. No details on the legal framework or the structure of the national cybersecurity system were provided, and no necessary resources were designated to fulfil the tasks, and no rights and obligations of the system co-participants were defined. Most importantly, no cyberspace emergency response procedures were prepared[60].

According to NIK, the engagement of government administration management, including the Prime Minister, was insufficient, which had a negative impact on the performance of tasks in the sphere of cybersecurity. This also adversely affected the resolution of controversies between individual agencies, and the cooperation between authorities and institutions engaged in state ICT security[61].

NIK identified only a few successful initiatives, including the appointment of CERTs by NASK, the ISA and the Ministry of National Defence, the development of a computer security incident response team at the Ministry of National Defence, and the establishment of the National Cryptology Centre, dissemination of guidelines and good practices as regards the protection of critical infrastructure by the Government Centre for Cybersecurity, and educational activities undertaken by NASK and the Police related to

[58] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.
[59] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[60] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.
[61] K.J. Jakubski**,** Analiza Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 *[An analysis of the Cybersecurity Strategy of the Republic of Poland for 2017-2022]* https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.

computer crime and cybersecurity. The adoption by the Council of Ministers of a national strategy for the management of threats in cyberspace was considered another positive aspect (Lisiak-Felicka, Szmit, 2016: 157).

NIK found that all the systems of individual audited entities failed to form a consistent uniform whole. The entities had separate, individual procedures for preventing threats in cyberspace[62].

NIK also found that the management of most of the audited entities, including the Minister of the Interior, responsible for security and crisis management, and the Minister of Administration and Digital Affairs in office at the time, responsible for coordinating activities in the field of IT security, were not aware of the tasks they had been entrusted with or the related obligations[63].

The Minister of Administration and Digital Affairs did not have the resources which would allow the actual performance of the mission related to the management of the national cyberspace protection system, and was not authorised to exert influence on other institutions which refused to cooperate or failed to fulfil their obligations accurately and on time.

The Minister of the Interior did not perform any tasks related to the development of the national cyberspace protection system. The operations of the Minister in the sphere of IT security were limited to the Ministry's own networks and systems, and yet even in this extent they were not duly performed.

The Supreme Audit Office noted that the provisions of the Telecommunications Law in force at the time had a fault in their structure, and could not be applied in practice for the purpose of fulfilling tasks related to IT security. This resulted in the fact that the President of the Office of Electronic Communications refrained from fulfilling the said obligations. These mainly consisted in obtaining data on incidents in cyberspace and informing the public about the threats arising from Internet use[64].

The crisis management system, controlled by the Government Centre for Security did not sufficiently account for new threats to the state's critical infrastructure, including the threats occurring in cyberspace. It is neither consistent with, nor complementary to, the activities in the sphere of ICT security.

The organisational units of the Police were actively involved in informing and educating the public about safe Internet use, and initiated measures related to combating computer

[62] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.
[63] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[64] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.

crime. However, the Commander-in-Chief of National Police failed to conduct diligent activities aimed at implementing a comprehensive and actual incident and cyberthreat response system within the Police structures.

The Minister of National Defence was actively involved in performing the tasks related to the development of the Ministry computer security incident response system, and took part in establishing the national cyberspace protection system[65].

The management of the ISA performed tasks related to the response to, and prevention of, computer security incidents in the systems of public administration entities, consisting in, i.a., the formation and maintenance of the CERT.GOV.PL team, and an early warning system called ARAKIS.GOV. The operations of the ISA were subject to significant restrictions, mainly resulting from insufficient resources and no formal powers granted to the CERT.GOV.PL team.

The management of NASK was undertaking numerous tasks, which were assessed by NIK as good practices in the sphere of cyberspace protection. They mainly included the establishment and maintenance of CERT Polska[66].

The framework of the system for financing activities related to the protection of Polish cyberspace has not been developed yet. No additional funds had been allocated for such activities, which in the view of NIK practically paralysed the operations of public entities in the scope of ICT security. The resources of individual audited entities were inadequate in relation to the obligations imposed on them.

No minimum legislative measures were undertaken aimed at regulating the issues related to the state's ICT security. No desired directions for legislative changes were outlined, and the legal regulations concerning cybersecurity, placed in various legal acts, were not inventoried. No assumptions of a normative act were prepared to define the structure of the national cyberspace protection system and its participants[67].

As noted by a representative of the Supreme Audit Office, the Poland does not have a functional national computer emergency response system in place. "Activities in the scope of incident response were carried out by CERTs operating independently from one another"[68]. Many entities do not have any comprehensive computer security incident response system in place, there are no CERTs, and incidents are not recorded. State administration management did not undertake any activities to work out the assumptions of the response team structure, establish information exchange channels and to designate

[65] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.
[66] Ibidem.
[67] Ibidem.
[68] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.

a national CERT, coordinating the activities of numerous entities, and being responsible for international cooperation. NIK called for the development of procedures regarding the notification of incidents, not only those that pose threat to personal data, but also other data processed in agencies (Lisiak-Felicka, Szmit, 2016: 156).

NIK found that the state administration lacked approximate knowledge of the range and type of incidents. The system of collection and recording such information turned out to be ineffective and futile. The prepared emergency response plans did not take into account threats coming from cyberspace. They only referred to conventional hazards such as natural disasters, and did not incorporate the change in the nature of threats resulting from, i.a., technological advancements"[69].

The existing legal regulations were not used to develop procedures in force in emergency situations related to cyberspace. The management of the entities did not see the need to take up efforts in this respect[70].

A substantial heterogeneity was found in the standards which form the foundations of the information security management systems (Lisiak-Felicka, Szmit, 2016: 157).

NIK analysed the activities undertaken by the ISA. The Agency, in cooperation with NASK, implemented a project consisting in the development, extension and maintenance of the early warning system ARAKIS.GOV. The operation of the system involved the installation of sensors in several dozen public institutions. The system sensors collected information on threats on the Internet. Unfortunately, the reach of the ARAKIS.GOV system, and the range of the data generated was limited. It resulted from the voluntary participation, shortage of funds as part of the project, and the installation of sensors only in public entities. The authorities have not provided a well-prepared, integrated and systemic state support for research in the sphere of cyberspace protection and the possibility of a matter-of-fact use of their results to improve ICT security[71].

The next of the NIK audits discussed in this chapter included the security of information and communication systems and the data stored in the systems. The Office audited selected entities using the Cobit 4.1 methodology for the assessment. The level of security assurance process management (maturity model) in the audited entities was expressed on a scale of zero to five, and can be described as: "defined" (3) – the Agricultural Social Insurance Fund; "repeatable but intuitive" (2) – Ministry of Justice, Ministry of Treasury,

[69] Ibidem.
[70] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.
[71] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.

the National Health Fund; "initial/ad hoc" (1) – Ministry of the Interior and the Border Guard[72].

According to NIK, data protection systems applied by the audited state entities did not ensure data security. The funds allocated for the development of the systems were insufficient. The activities aimed at ensuring system security were often sluggish. A risk was posed that the operation of information and communication systems which are vital for the functioning of the state, might be disrupted. Information security management should not be performed without procedures, indicators or plans in this respect[73].

The level of development and implementation of the Information Security System in the audited entities did not guarantee an acceptable security level of data stored in information systems used to perform vital public tasks. Information security processes were implemented in a chaotic and intuitive way[74].

In all the audited entities, apart from the Agricultural Social Insurance Fund, such activities were based on simplified and informal rules established on the basis of existing good practices and experience of IT department employees[75]. The Information Security Management System was in place only at the Agricultural Social Insurance Fund. Only this institution officially had all processes required for data safety assurance in place. All the activities were performed with a view to obtaining the ISO 27001 certification by the Agricultural Social Insurance Fund. As regards the remaining audited entities, the activities were modelled on informal and simplified rules arising from good practices and the experience of the IT department staff. Ad hoc measures did not guarantee a proper, reliable and cohesive data security governance.

The audit results in this area showed, i.a.: 1) the lack of required analytical studies and procedures (including those concerning incidents, task identification, anti-virus software distribution); 2) failure to implement information security management systems; 3) lack of data safety assurance plans; 4) a limited scope of supervision, testing and monitoring of security[76].

Another issue subject to NIK audit was risk identification. The audited entities limited the application of methods for the monitoring and identification, and prevention of risk related to the security of information processed in information and communication

[72] G. Stech:, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[73] https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-o-bezpieczenstwie-danych.html.
[74] Ibidem.
[75] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[76] https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-o-bezpieczenstwie-danych.html.

systems. The Office found that risk assessment activities were undertaken only occasionally, and there were no procedures in this respect[77].

Based on the requirements arising from the obligations related to the operation of critical infrastructure, laws governing confidential information protection, and the implementation of the Cyberspace Protection Policy, the process was managed only in a minimum scope only in three of the audited entities. The identification of assets, the definition of their values and the selection of the methodology should be preceded by comprehensive risk assessment. The assessment of risks and costs required for mitigating their impact should be a basic task performed by persons responsible for the security of data processing systems[78].

There was a substantial discrepancy between the efforts taken for the protection of specified individual information categories, i.e. information subject to statutory protection (classified information and personal data) and other information, whose protection was not expressly laid down in legal regulations, but which has a huge significance for the proper performance of essential tasks by the entities. The audited entities were also not aware that, in addition to information protected by law, there is also information which is important and should be protected in the same way. In contrast to the specific normative requirements for the protection of classified information and personal data, the identification of other vital information and the selection of procedures for its protection is basically left to information holders[79].

NIK also found that none of the audited entities defined the scope of responsibility of individual employees as regards to ensuring data security. This resulted in frequent disputes related to competence issues. IT units were often entrusted with all the issues concerning information security[80]. This resulted in limiting the actual scope of information protection solely to information systems and data storage media. Due to competence issues, this approach hindered the possibility to build information protection systems covering entire institutions, disregarding the common truth that a security system is as strong as its weakest link. In most of the audited entities security assurance processes were performed by external companies. No efforts were made with a view to managing the related risks[81]. Moreover, the management of the institution, in some ways "delegating the issue to be addressed" to a specialist unit, failed to sufficiently accept their role in the development and attainment of strategic goals related to information security. Appointed coordinators (usually individual persons) were basically responsible for guaranteeing

[77] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[78] https://www.nik.gov.pl/aktualnosci/bezpieczenstwo/nik-o-bezpieczenstwie-danych.html (May 26, 2017).
[79] Ibidem.
[80] G. Stech, http://www.computerworld.pl/news/NIK-Cena-za-cyberbezpieczenstwo-bedzie-wysoka,407735.html.
[81] Ibidem.

information security. They had no sufficient capabilities and powers to pursue activities in the sphere of coordinating tasks and management.

To summarise the analysis of the results of audits carried out by NIK, it can be stated that there was a risk of disruption of the operations of communication and information systems critical to the functioning of the state, and that the data stored in the systems might be intercepted by unauthorised persons. The main factor hindering active state operations in the IT sphere is the lack of system-based approach to cybersecurity. The activities are conducted occasionally, and are dispersed. The system lacks a single decision-making centre coordinating operations in other public institutions. No basic threats to the domestic ICT infrastructure were identified. No national cyberspace protection strategy was developed. No procedures for the response to cybersecurity incidents was prepared. Most of all, there are no necessary legal regulations and financial instruments to implement plans and strategies related to the protection of the Polish cyberspace. The second audit, covering the security of communication and information systems, and the data stored in such systems, showed that the audited state authorities applied data protection systems which failed to ensure effective safeguards. The funds allocated for the development of the systems were insufficient. The Information Security Assurance System in the audited entities did not guarantee an acceptable security level of data stored in information systems.

Polish cyberspace needs state-of-the-art institutions, people with a vision of the future, and professional and coordinated actions with a view to ensuring the security of society and the state.

5 Documents shaping the status of Polish cybersecurity

Virtual cyberspace and the information sphere have become an area for operations of great potential, consequently transforming into a battlefield of enemy forces "devoid of geographical parameters, unmeasurable, and unlimited."[82] It is also a test for the security of Polish cyberspace. The security can be defined as a process of ensuring a safe functioning of the state cyberspace as a whole, of its structures, its natural and legal persons including enterprises and other entities without legal personality, and other bodies holding their communication and information systems and information resources in global cyberspace at their disposal[83].

Since 2008, the Ministry of the Interior and Administration of the time, and, i.a., the ISA, were carrying out comprehensive preparations for the development of the strategy for

[82] Wizja Sił Zbrojnych RP – 2030 *[The Vision of the Polish Armed Forces 2030]*, Warsaw 2008, pp. 13-14, http://www.znp.wat.edu.pl/images/stories/ Wizja_SZRP_2030.pdf.
[83] Doktryna Cyberbezpieczeństwa RP *[Cybersecurity Doctrine of the Republic of Poland]*, Warsaw 2015, https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html.

counteracting threats in cyberspace[84]. In order to ensure the security of the Republic of Poland in cyberspace, two essential documents were drafted – the Government Cyberspace Protection Programme of the Republic of Poland for the years 2011-2016[85] ("the Programme") and the Cyberspace Protection Policy of the Republic of Poland[86] ("the Policy"), which constituted the grounds for the process for the protection of Polish cyberspace, and the development of legal solutions in this respect (Kowalewski, Kowalewski, 2014).

In 2010, the Programme became the essential document which addressed all the problems related to the protection of Polish cyberspace in a concise way. The document allowed the achievement of the objectives of the EU Digital Agenda for Europe[87], and it also referred to the cooperation with the European Union, in particular with the European Agency for Cybersecurity, ENISA, and to the collaboration with the governments of other EU Member States[88].

The subject of the Programme was to put forward a proposal for educational, technical, legal and organisational measures, with a view to expanding the capacity to combat and prevent threats in cyberspace. The strategic objective of the Programme was to guarantee a sustainable cybersecurity of the state. The development of organisational and legal framework and the configuration of an effective cooperation in the sphere of information exchange between public administration and other entities and users of Polish cyberspace, including enterprises, facilitated the achievement of the strategic objective.

The Programme assumed the following detailed objectives: 1) defining the authority of entities responsible for the protection of cyberspace; 2) developing and implementing a cybersecurity management system which is consistent for all public administration entities, and establishing guidelines in this respect, applicable to private entities; 3) mitigating the impact of interference with cybersecurity; 4) launching a stable cooperation and information exchange system in entities responsible for the protection of cyberspace, the operators of critical ICT infrastructure, and enterprises providing services in cyberspace; 5) improving the quality of ICT infrastructure security, including the

[84] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.
[85] The Government Cyberspace Protection Programme of the Republic of Poland for the years 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.
[86] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.
[87] The Government Cyberspace Protection Programme of the Republic of Poland for 2009-2011 was adopted in March 2009 and it was intended as a draft programme for 2011-2016, Warsaw 2009.
[88] The Government Cyberspace Protection Programme of the Republic of Poland for 2009-2011. Principles, Warsaw, March 2009. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_ Strategy.pdf.

state's critical ICT infrastructure; 6) raising the awareness of users in the field of cybersecurity methods and measures[89].
The objectives of the Programme were meant to be implemented by: 1) putting in place, on a mass scale, in public administration entities and private entities, mechanisms aimed at the early detection and prevention of threats to cybersecurity, and a proper procedure in the event of confirmed incidents; 2) conducting large-scale education activities in the field of Polish cyberspace protection addressed to the public, and specialist training, 3) establishing a system for the coordination of preventing and responding to cyber attacks and threats in cyberspace, including cyber-attacks of a terrorist nature[90].

The Policy is addressed to all the cyberspace users within the State and beyond its territory, in places where the representatives of the Republic of Poland operate (diplomatic posts, military contingents).

The Council of Ministers was the authority responsible for supervising the implementation of the Programme. The Minister of the Interior and Administration, acting on behalf of the Council of Ministers, was the authority responsible for carrying out the Programme. The Minister, through his office, was to manage an Inter-Ministry Polish Cyberspace Protection Team[91].

The Programme identified necessary measures for the introduction of corporate and legal governance, allowing the implementation of Polish cyberspace protection mechanisms, with a time framework provided for such actions. Meanwhile, the course of the protection of ICT resources was treated as a continuous process, vital from the perspective of the functioning of the state, and thus not limited by any programme completion date.

The Policy outlined a similar objective[92]. It was a document whose contents were equivalent to the aforementioned Government Programme, and with different variants of national security strategies being implemented at the European Union and national levels (Kowalewski, Kowalewski, 2014).

The Government Programme, which was the outcome of cooperation between the Ministry of Administration and Digital Affairs[93] of the time and the Internal Security Agency, was adopted on 25 June 2013. At the time, it was one of the key documents, in

[89] The Government Cyberspace Protection Programme of the Republic of Poland for 2011-2016 http://bip.msw.gov.pl/bip/programy/19057,Rządowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html.
[90] Ibidem.
[91] Ibidem.
[92] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.
[93] The Ministry was responsible for Polish information and communication policy, the growth of the information society, and public cyberspace protection projects.

which government administration expressed their approach to the implementation of a coordinated network and information security process in this country[94].

The document listed areas and solutions aimed to provide cybersecurity. They referred to the government administration sphere. The Programme did not indicate any authorities responsible for the fulfilment of the tasks listed in the document[95].

According to the Policy, the strategic objective was to achieve an acceptable level of cyberspace security of the state, and the actions undertaken to achieve the strategic objective were meant to be the result of risk assessments conducted by qualified entities, with respect to threats occurring in cyberspace. As for risk management, the Policy focused on collecting information, suggesting only in small extent what activities at strategic level, in particular those related to budget spending, were to be undertaken based on status reports which were to be submitted to the Minister competent for computerisation by the end of January each calendar year. The reports should include general data relating to the hazards, risks, and vulnerabilities identified in each of the sectors in which an individual institution operates and for which it is responsible. They should contain information on risk management methods[96].

The next document which devoted relatively substantial space to cybersecurity was the National Security Strategy of the Republic of Poland 2014[97] ("the Strategy"). According to the document, "ensuring safe functioning of the Republic of Poland in cyberspace" is one of the strategic goals in the sphere of security (Bogdół-Brzezińska, Gawrycki, 2003: 51). New threats to state security listed in the Strategy include: "cybercrime, cyberterrorism, cyber espionage and cyber conflicts, with the participation of non-state entities, and cyber war understood as a confrontation between countries in the cyberspace." Such trend was explained by an increasing dependency on information and communication technologies (Kowalewski, Kowalewski, 2014).

The solutions aimed at enhancing the capability for defensive and offensive activities in the sphere of cybersecurity, as outlined in the Strategy, include[98]: 1) conduct of information warfare in the cyberspace; 2) development and use of appropriate procedures for social communication in this area; 3) cooperation and coordination of protective actions with entities from the private sector (in particular the finance, energy, transport, telecommunications and health care sectors); 4) identification and prevention of offences

[94] M. Stempień, http://docplayer.pl/15658274-Ochrona-cyberprzestrzeni-rzeczpospolitej-polskiej-a-wspolpraca-panstw-czlonkowskich-unii-europejskiej-marta-stempien-8.html.
[95] Cyberspace Protection Policy, Warsaw, 25 June 2013 https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf.
[96] Ibidem.
[97] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej *[National Security Strategy of the Republic of Poland]*, BBN 2014, p. 19. https://www.bbn.gov.pl/ ftp/SBN%20RP.pdf.
[98] M. Stempień, http://docplayer.pl/15658274-Ochrona-cyberprzestrzeni-rzeczpospolitej-polskiej-a-wspolpraca-panstw-czlonkowskich-unii-europejskiej-marta-stempien-8.html.

committed in cyberspace and prosecution of their perpetrators; 5) conduct of preventive activities with regard to threats in cyberspace; 6) allied cooperation, also at the level of operational activities aimed to actively combat cybercrime, including the exchange of experience and good practice in order to increase the efficiency and effectiveness of domestic measures[99].

Another document which included cyberspace in its vision was the Cybersecurity Doctrine of the Republic of Poland ("the Doctrine"), constituting an implementing document in relation to the Strategy, was published on 22 January 2015. According to the document, Poland endeavours to fully exploit the achievements of the North Atlantic Treaty Organization and the European Union in the sphere of cyberspace protection. The objective was to create conditions for joining and providing a strategic direction of the efforts for the development of an integrated cybersecurity system of the Republic of Poland[100].

The strengthening of Polish cybersecurity is the result of the potential coming from Poland's membership in allied defence and protection structures. Properly taking advantage of the opportunity should result from not only the engagement in the works of international organisations, including the European Union and the activities as part of cybersecurity agendas, but also from Poland's bilateral cooperation with the Member States whose structures are more advanced in matters related to cyberspace protection[101].

The Cybersecurity Doctrine marked out strategic directions for activities aimed to ensure the security of the Republic of Poland in cyberspace. It should also be treated as a uniform concept foundation, providing a comprehensive and concise approach to the issue of cyber defence and cyberspace protection – as a common denominator for activities performed by security and public order services, public administration bodies, citizens and the private sector. Thanks to this, the Cybersecurity Doctrine could constitute a starting point for further efforts to boost the security of Poland[102].

The document recommended the state administration to align all their strategic documents concerning cyberspace security as soon as possible. The target model would be to draw up a single document, a cyberspace protection strategy of the Republic of Poland, which would have a function similar to other documents of the type developed in other countries[103].

---

[99] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej *[National Security Strategy of the Republic of Poland]*, BBN 2014, p. 35. https://www.bbn.gov.pl/ ftp/SBN%20RP.pdf.
[100] M. Stempień, http://docplayer.pl/15658274-Ochrona-cyberprzestrzeni-rzeczpospolitej-polskiej-a-wspolpraca-panstw-czlonkowskich-unii-europejskiej-marta-stempien-8.html.
[101] Doktryna Cyberbezpieczeństwa RP *[The Cybersecurity Doctrine of the Republic of Poland]*, Warsaw 2015. https://www.bbn.gov.pl/pl/prace-biura/publikacje/6818,Doktryna-cyberbezpieczenstwa-RP.html.
[102] Ibidem.
[103] Ibidem.

The current vision of the development of security in cyberspace is the Cybersecurity Strategy of the Republic of Poland for 2017-2022[104], which is a continuation of undertakings previously made by the government administration. It is also a concept and implementing document in relation to the Strategy. The document was prepared by an inter-Ministry group, composed of the representatives of the Ministry of Digital Affairs, Ministry of the Interior and Administration, the Government Centre for Security, the Internal Security Agency, NASK and the National Security Bureau. It was approved by the Council of Ministers Committee for Digital Affairs, referred to the Government for debate, after which it was adopted by way of a resolution[105].

The fundamental objective of the document is to guarantee a high level of security in the public sector, the private sector and for citizens in the scope of providing and using essential and digital services. Within the next five years, Poland is to become resilient to cyber attacks and have a rapidly developing digital economy. The document mentions the need to have offensive capabilities in cyberspace.

The assumption behind the new strategy is to define the operation sphere, aimed at achieving a high level of resilience of national communication and information systems, critical infrastructure operators, digital service providers, operators of essential services and public administration[106]. Such operation method will allow Poland to become a country resilient to the threats and attacks arising from the use of cyberspace by 2022. The Polish cyberspace, thanks to the synergy of internal and international-level activities, will become a safe environment providing a possibility to perform all state tasks and functions. This will allow the exploitation of the full potential of digital economy, while respecting the rights and freedoms of citizens[107]. The provisions of the new strategy indicate a wide range of protection. The Polish government is also planning to ensure the security of private sectors. The strategy also assumes the increased effectiveness of law enforcement and judicial authorities in investigating and combating crime and acts of an espionage or terrorist nature in the cyberspace. The primary objective is to be achieved through four specific objectives.

The first specific objective – to achieve capability for nationally coordinated action to prevent, detect, fight, and mitigate the consequences of incidents that compromise the security of the state's critical communication and information systems – is to be achieved by: 1) enhancing the ICT security of essential and digital services and critical

[104] https://mc.gov.pl/files/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017-2022.pdf.
[105] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.
[106] A. Kozłowski, Bezpieczna Polska w cyfrowej erze *[Secure Poland in the Digital Age]*, http://www.cyberdefence24.pl/555852,bezpieczna-polska-w-cyfrowej-erze-strategia-cyberbezpieczenstwa-na-lata-2017-2022-analiza.
[107] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.

infrastructure; 2) adapting the legal environment to the needs and challenges in the area of cybersecurity – implementing the NIS Directive to Polish legislation; 3) improving the effectiveness of cooperation between entities responsible for the security of cyberspace in the Republic of Poland – consolidating and harmonising the actions taken by all entities; 4) guaranteeing a secure supply chain, which covers subsystems entailing the storage, production, distribution, transport, storage and recycling of components of communication and information systems; 5) improving the structure of the national cybersecurity system; 6) preparing and implementing a risk management system at national levels – developing a concise risk assessment methodology, taking into account the specific nature of individual sectors, essential services, digital service providers and operators of critical infrastructure; 7) building procedures for warning cyberspace users about risks stemming from cyberthreats[108].

The second specific objective – enhancing the capacity to counteract cyber threats – is to be achieved by: 1) gaining the capacity to perform a full spectrum of military operations in cyberspace, including counteracting sources of threats; 2) enhancing the capacity to counteract cybercrime, including cyber espionage and incidents of a terrorist nature, occurring in cyberspace – information exchange, international cooperation and better coordination between various institutions; 3) building a secure communication system for the purposes of national security; 4) building capacity in the area of threat analysis at the national level – the establishment of an analysis centre, whose mission will be carried out by the National Cybersecurity Centre[109].

The third specific objective – increasing the national potential and competence in the area of security in cyberspace – will be achieved by 1) development of industrial and technological resources for the purposes of cybersecurity – boosting the national potential through R&D activities in the sphere of ICT security, covering the operations of the National Centre for Research and Development; 2) building cooperation mechanisms between the public sector and the private sector; 3) increasing the competence of the staff of entities relevant to the functioning of cyberspace security – education at expert level and training of state administration staff; 4) creating conditions for the safe use of cyberspace by citizens – education and awareness raising in relation to threats arising from the virtual world[110].

The fourth specific objective – positioning the Republic of Poland as a strong international player in cybersecurity – is to be achieved by: 1) active international cooperation at the technical and operational level – developing joint procedures for action as part of the EU, NATO and V4 group, joining various international CSIRT networks; 2) active international cooperation at the strategic and political level – as part of NATO,

[108] Ibidem.
[109] Ibidem.
[110] Ibidem.

the UN, the Visegrád Group, or cooperation with the countries of the Baltic Sea Region"[111].

The Cybersecurity Strategy was adopted for a period of five years. The document identifies the Ministry of Digital Affairs as the entity responsible for synchronising the actions of institutions at a strategic level. As regards to the operational level, emphasis was placed on the significance of NC Cyber and the National CSIRT, and on the need to develop them. The new document is consistent with the provisions of the NIS Directive[112]. It is also worth noting the obligation to review and evaluate the effects of the Strategy two years after its adoption and in the fourth year of its application, with the evaluation results to be submitted to the Council of Ministers[113]. Each year, the Minister of Digital Affairs is to prepare a report on the progress in implementing the Strategy. Within 6 months of the Strategy's entering into force, an "Action Plan for the implementation of the Cybersecurity Strategy" will be prepared, together with estimated strategy implementation costs. Moreover, there are plans to utilise the resources of the National Centre for Research and Development and, where possible, EU funds[114].

In conclusion, it should be clearly stated that the Cybersecurity Strategy of the Republic of Poland explores the most important topics which can be found in similar documents of other countries, and creates a good basis for further action. One of the methods is to act upon the detailed objectives in the "Action Plan for the implementation of the Cybersecurity Strategy" being developed by the Minister of Digital Affairs in cooperation with other members of the Council of Ministers, the managers of central government agencies, and the Director of the Government Centre for Security. The introduction of the documents will facilitate the commencement of synchronised work on individual detailed areas and on cybersecurity law.

Thanks to all the documents shaping Polish cyberspace and the resulting activities, in 2022 Poland will be able to become a country which is more resilient to attacks and threats from cyberspace. Opportunities will be provided to exploit the potential of digital economy, perform all state functions in a safe way and efficiently perform public tasks related to cybersecurity.

---

[111] Ibidem.
[112] A. Kozłowski, http://www.cyberdefence24.pl/555852,bezpieczna-polska-w-cyfrowej-erze-strategia-cyberbezpieczenstwa-na-lata-2017-2022-analiza.
[113] K. J. Jakubski, https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/.
[114] A. Kozłowski, http://www.cyberdefence24.pl/555852,bezpieczna-polska-w-cyfrowej-erze-strategia-cyberbezpieczenstwa-na-lata-2017-2022-analiza.

References

Adamski A. (2005) Cyberprzestępczość – aspekty prawne i kryminologiczne, *Studia Prawnicze*, 167(4), pp. 51-76.

Broderick, J. S. (2001) Information Security Risk Management – When Should It be Managed?, *Information Security Technical Report*, 6, pp. 12-18.

Białas, A. (2006) *Bezpieczeństwo Informacji i usług w nowoczesnej instytucji i firmie* (Warsaw: WNT).

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

Bógdoł–Brzezińska, A. & Gawrycki, M. F. (2003) *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie* (Warsaw: OW ASPRA-JR).

Burdziak, A., Cieślak Ł. & Rodzewicz P. (2011) *Technologia informacyjna dla prawników* (Wrocław: Prawnicza i Ekonomiczna Biblioteka Cyfrowa).

Chałubińska–Jentkiewicz, K. (2014) Bezpieczeństwo cyberprzestrzeni jako zadanie publiczne w systemie bezpieczeństwa narodowego RP, *Zeszyty Naukowe AON*, 3(2), pp. 20-35.

Chałubińska-Jentkiewicz, K. & Karpiuk M. (2015a) *Informacja i informatyzacja w administracji publicznej* (Warsaw: AON).

Chałubińska-Jentkiewicz, K. & Karpiuk M. (2015b) *Prawo nowych technologii. Wybrane zagadnienia* (Warsaw: LEX, a Wolters Kluwer business).

Crapko, M. (2012) *CMMI, Doskonalenie procesów w organizacji* (Warsaw: PWN).

Czyżak, M. (2009) Spamming i jego karalność w polskim systemie prawnym, *Pomiary. Automatyka. Kontrola*, 7, pp. 548-551.

Feret, E. (2020) Legal Security and Financial Security of Local Communities. Selected Issues, *Studia Iuridica Lublinensia*, 29(1), pp. 85-98, http://dx.doi.org/10.17951/sil.2020.29.1.85-98.

Gillies, A. (2011) Improving the quality of information security management systems with ISO27000, *TQM Journal*, 23, pp. 367-376.

Grzelak, M. & Liedel, K. (2014) Bezpieczeństwo w cyberprzestrzeni, zagrożenia i wyzwania dla Polski – zarys problem, *Zeszyty Naukowe Uniwersytetu Ekonomicznego*, 2(926), pp. 125-139.

Gogołek, W. (2007) Manipulacja w sieci, In: Siemienicki, B. (eds.) *Manipulacja, media, edukacja*, (Toruń: Adam Marszałek).

Hone, K. & Eloff, J. H. P. (2002) Information security policy – what do international Information security say?, *Computers and Security*, 21, pp. 402-409.

Hołyst, B. (1996) *Kryminalistyka, wydanie VIII* (Warsaw: Wydawnictwo Prawnicze PWN).

Humphreys, E. (2007) *Implementing the ISO/IEC 27001 Information Security Management System Standard* (Norwood: Artech House).

Karpiuk, M. (2015) Odmowa wydania poświadczenia bezpieczeństwa przez polskie służby ochrony państwa, *Secretum*, 2, pp. 137-147.

Karpiuk, M. (2018) Miejsce bezpieczeństwa osobowego w systemie ochrony informacji niejawnych, *Studia nad Autorytaryzmem i Totalitaryzmem*, 1, pp. 85-99.

Karpiuk, M. & Chałubińska-Jentkiewicz K. (2015) *Prawo bezpieczeństwa informacyjnego* (Warsaw: AON).

Kisielnicki, J. (2008) *MIS. Systemy informatyczne zarządzania* (Warsaw: Placet).

Kitler, W. (2011) *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system* (Warsaw: AON).

Kosiński, J. (2015) *Paradygmat Cyberprzestępczości* (Warsaw: Difin).

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

Kreft, K. (2010) Normy, standard, modele i zalecenia w zarządzaniu bezpieczeństwem informacji, *Współczesna Gospodarka*, 1, pp. 1-11.
Liderman, K. K. (2002) *Bezpieczeństwo teleinformatyczne* (Warsaw: School of Applied Computer Science and Management).
Lisiak–Felicka D. & Szmit M. (2016), *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia* (Kraków: EAS).
Matuszczyk A. & Matuszczyk P. (2006) *Instrumenty bankowości elektronicznej* (Warsaw: CeDeWu).
Murdoch, A. (2003) *Komunikowanie w kryzysie. Jak ratować wizerunek firmy* (Warsaw: Poltext).
Nowicki A. & Unold J. (eds.) (2002) *Organizacyjne aspekty doskonalenia systemów informacyjno–decyzyjnych zarządzania* (Wrocław: Wydawnictwo AE).
Paprzycki L. K. & Rau Z. (2009) (eds.) *Praktyczne elementy zwalczania przestępczości i terroryzmu* (Warsaw: Wolters Kluwers).
Pilawski, B. (2000) *Bankowość elektroniczna – meandry i zawirowania. Zastosowanie rozwiązań informatycznych w instytucjach finansowych. Materiały konferencyjne* (WBK S.A.).
Radoniewicz, F. (2016) *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko bezpieczeństwu danych komputerowych i systemów informatycznych* (Warsaw: Wolters Kluwer).
Radoniewicz, F. (2019) Wprowadzenie, In: Kitler, W., Taczkowska-Olszewska, J. & Radoniewicz (ed.) *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz* (Warsaw: C.H. Beck).
Schjolberg, S. (1983) *Computers and Penal Legislation – A Study of the Legal Politics of a new Technology* (Oslo: Universitetsforlaget).
Szczepaniuk, E. (2016) *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprzestrzeni państwa* (Warsaw: ASW).
Świątkowska J. & Bunsch I. (2011) *Cyberterroryzm, nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku* (Warsaw: Wydawnictwo Instytutu Kościuszki).
Wawrzyniak, D. (2002) *Zarządzanie bezpieczeństwem systemów informatycznych w bankowości* (Warsaw: OW Zarządzanie i Finanse).
Wojciechowska-Filipek, S. & Ciekanowski, Z. (2016) *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki – organizacji – państwa* (Warsaw: CeDeWu).
Wojtaszek, K. & Materska–Sosnowska, A. (2009) *Bezpieczeństwo państwa. Wybrane problemy* (Warsaw: Oficyna Wyd awnicza ASPRA-JR)..
Żukrowska, K. & Grącik, M. (2006) *Bezpieczeństwo międzynarodowe. Teoria i praktyka* (Warsaw: SGH).