The Functioning of State Power Structures and Cybersecurity

Marzena Toumi

Abstract The national security of Poland in the twenty-first century is strongly influenced by the processes taking place in the contemporary global security environment. These changes are characterised by high dynamics and complexity as well as the occurrence of asymmetric threats, among which the most dangerous are threats in cyberspace. The functioning of the state and the implementation of its constitutional obligations are increasingly dependent on the development of modern technologies, the information society and the smooth functioning of cyberspace, which is largely dependent on the security of the ICT infrastructure, which allows the use of cyberspace, information resources and services accumulated therein. Rapid progress in the field of digital technologies necessitates the effective use of the latest technologies while creating an opportunity for the Polish state to leave the role of only a user and join the group of countries with an effectively functioning digital economy, providing solutions and co-creating international standards. To meet these expectations, the President of the Republic of Poland signed the Act on the National Cybersecurity System on 1 August 2018, implementing Directive 2016/1148 (NIS Directive).

State power is a form of universal or general power over the whole population in a given territory. It is exercised by a special power apparatus elected from among society as a whole.

In the literature on the subject matter, the features of state power include its primary character, indivisibility, permanency, exercisability under legal regulations, implementation only in an organised manner, the possibility to legally use coercive measures (also direct), and exercisability in a given territory.[1]

[1]Representatives of state power, in order to gain citizens' endorsement, use various arguments which are meant to legitimise their powers. These arguments pertain both to the sources of power

M. Toumi (✉)
Instytut Prawa/Institute of Law, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: m.toumi@akademia.mil.pl

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_10

State authority in a democratic system has a collective character, as it comprises both direct state authority and social (ultimate) authority.

Direct authority is composed of the political personnel of state bodies and public servants (bureaucracy). The managing bodies of a state organisation, political parties, interest groups, and mass media, constitute the power elite. Direct state authority ensures both internal and external security, protects socio-economic relations, and creates the conditions conducive to self-assembly, e.g. through social governance. Social authority is exercised by the nation, i.e. all citizens who participate in electing the political leadership and influencing its rule.

State authority can, therefore, be said to jointly cover the power elite and the nation. There is no single sovereign entity which would finally and ultimately decide on the ways state power should be exercised (the rule of the people exercised by the elites they elect).

The major powers vested in state authority include legislative powers, i.e. the powers to enact universally binding legal regulations under the Constitution, i.e. without violating any constitutional civic rights and freedoms; to take measures to amend the obligations arising from already enacted regulations (administrative decisions made by the government, general administration, and specialised services); and to impose sanctions on those infringing the legal regulations (via the judiciary and direct coercion bodies, such as the army, the police, and the prison service).

The bodies vested with decision-making powers constitute the state power apparatus, i.e. a system of state bodies, interrelated in terms of organisation, along with offices and institutions which serve the central decision-making authority (e.g. the government) in implementing current state policies.[2]

State power should fulfil the following four core functions: integrative, distributional, security-making, and structure-building. This article focuses, in particular, on the third function.

One of the duties of state power is, therefore, to create a "security umbrella", to protect those who fall within the impact of the state's decision-makers and

(legal power) and also, increasingly, to the ways in which it is exercised (efficient and competent) as well as to the consequences of their actions (successful, meeting social needs), cf. Kuciński (2008), p. 113.

[2]The state apparatus includes (1) legislative bodies (the Sejm and the Senate) (2) executive bodies (the President and the Council of Ministers), which are entrusted with performing state duties aimed at implementing the Law. government administration authorities are also endowed with executive power. The National Broadcasting Council, whose powers are provided for in the Constitution of the Republic of Poland, is also an executive body, and has the right to issue regulations. In the Election Code, the National Electoral Commission was appointed as the *sui generis* executive body (although its powers are not provided for in the Constitution of the Republic of Poland, and it does not have the right to issue regulations, it may issue instructions binding on lower-level electoral bodies) (3) coercion bodies (e.g. the police, the army)—a group of state bodies whose aim is to ensure the implementation of the Law. They are in charge of maintaining public order, as well as of ensuring the external and internal security of the country (4) judicial bodies—the Supreme Court, common courts, military courts, and administrative courts (5) inspection bodies (e.g. the Supreme Chamber of Control) which supervise compliance with the Law.

authorities. The latter fulfil their security functions by employing various decision-making tools, and with a considerable use of legal instruments.[3]

The national security system is understood as the entirety of resources, means, and forces (entities) earmarked by the state for the performance of tasks in the field of security, organised (into subsystems and components), maintained and prepared in a manner capable of fulfilling the purpose of performing such tasks.[4] The objective of the National Security Strategy is to counteract emerging threats to the survival of both the nation and the state, to territorial integrity, to political independence and sovereignty, to the efficient functioning of state institutions, and to socio-economic development. It covers elements of both external and internal security, oriented towards ensuring nationwide security in combination with the socio-economic development of the country.[5]

The national security system comprises all the bodies and institutions constituting legislative, executive, and judicial powers, which are in charge of ensuring security in the light of the Constitution of the Republic of Poland and other relevant acts. These include Parliament, the President of the Republic of Poland, the President of the Council of Ministers, the Council of Ministers, central government administration authorities, and other central state bodies and public institutions. The armed forces, as well as government services and institutions, also form crucial elements in the national security system. They are obliged to prevent and counteract external threats, to ensure public security, to conduct rescue operations, and to protect people and property in extraordinary situations. In addition, the system covers local government authorities and other legal entities, including entrepreneurs who form the industrial defence potential, and implement duties in the field of national defence.

The national security system consists of the national security control subsystem, and several executive subsystems. The control subsystem is formed by public authorities and managers of organisational units implementing duties related to national security, and command authorities of the Armed Forces of the Republic of Poland. Executive subsystems are the means and forces earmarked for the Ministers leading government administration departments, central-government administration authorities, province governors (voivodes), local government authorities, and other public institutions and entities responsible for implementing duties in the field of national security as arising from the applicable Acts.[6]

Processes occurring in the contemporary global security environment have a material impact on the national security of Poland in the twenty-first century. These are characterised by powerful dynamics and complexity of changes, and by the emergence of asymmetric threats, the most serious including terrorism, the

[3] Kuciński (2008), pp. 108–109.

[4] *The White Book on the National Security of the Republic of Poland*, Warsaw 2013, p. 36.

[5] *The Strategy of the Development of the National Security System of the Republic of Poland 2022 (2013)*, adopted by way of Resolution No. 67 of the Council of Ministers of 9 April 2013, Journal Monitor Polski 2013, item 377.

[6] Dubiel (2018), Accessed on 20 September 2020.

proliferation of weapons of mass destruction and the means of their delivery, international organised crime, and threats in cyberspace.[7] The functioning of the state and the performance of its constitutional duties increasingly depends on the development of modern technologies, the information society, and the uninterrupted functioning of cyberspace. The last of these, in turn, is largely dependent on the security of the communications infrastructure which facilitates the use of cyberspace, and of information resources and services which function within it.

Cyberspace is understood as "a space for the processing and exchange of information created by information and communication systems," as defined in Article 3 (3) *of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks,*[8] "including the links between them and their relations with users." Virtual space also tends to be increasingly treated as the territory of a given country. The cyberspace of the Republic of Poland is the cyberspace within the territory of Poland and outside, and basically covers any places where representatives of the Republic of Poland operate (e.g. diplomatic posts or military contingents).[9]

In the contemporary world, cyberspace is a major channel of information exchange, and the issues of electronic data transfer are increasingly pertinent to public institutions.[10] This is due to the progressing digitisation of offices and public institutions, as a result of which the computerisation of office infrastructures is triggering the growing use of information technologies in the electronic collecting, processing, and transferring of confidential information between entities in the national economy. This also involves the computerisation of the processes utilising the resources of the personal data of the customers served by these economic entities, and of citizens' data available to offices and public institutions.[11]

As part of the state's digitisation process, such technologies are used by public institutions (government and local government administration institutions, as well as legislative, executive, and judicial bodies), specialised services (e.g. the police, the emergency services, and the fire service), and media, banking, and finance institutions as part of their service portfolios, transport (by air and rail), and energy and

[7] *The Strategy* .... (2013), p. 4.

[8] Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks, consolidated text Polish Journal of Laws of 2020, item 346, as amended.

[9] *The Cyberspace Protection Policy of the Republic of Poland*, a document adopted by the Ministry of Administration and Digitisation and the Internal Security Agency (2013), Warsaw, p. 5. Such a definition of the cyberspace of the Republic of Poland does not cover the storage and processing of information, e.g., in a cloud, which is not necessarily located within the Polish territory. This provision is exclusive of new technologies, e.g. data storage in Azure, AWS (cf. *The Cyberspace Protection Policy of the Republic of Poland (departmental comments by ISSA Poland)* in: http://mac.gov.pl/wp-content/uploads/2012/09/polityka-CBR-stan-na-18-09-2012-konsultacje-resortowe-.pdf, accessed on 10 October 2020.

[10] Borkowski (2013), pp. 112–134.

[11] Gołębiowska (2015), p. 29.

water supply networks.[12] Most of these fields form part of the so-called critical infrastructure, which is understood as a network of interrelated systems enabling public, economic, and social institutions to fulfil their basic duties, such as maintaining security and public order, and rendering core social services.[13]

The use of e-government[14] brings numerous benefits both for the administration system itself, such as improved communication (both internal and external), and increased operational transparency, which results, *inter alia*, from services standardisation and procedures automation (eliminating the human factor), and for individual citizens and society—a faster and more efficient handling of official matters increases customer satisfaction and contributes to building a positive image of public administration. E-government provides employees with easier access to information and facilitates information exchange, both within a unit (a given office) and between various units. It also makes it quicker to gather (in one place) voluminous information regarding an entity (e.g. its public-law obligations; tax arrears or no tax arrears; payments of premiums to the Social Insurance Institution, etc.), which then facilitates prompt verification of the information (data) submitted to the institution, and, in consequence, the prompt detection of irregularities, and, where necessary, the instituting of explanatory proceedings.[15]

In compliance with the provisions included in the government's strategic document *The Strategy for Responsible Development,* adopted by the Council of Ministers in 2017, e-government was seen as a factor determining a well-functioning state.[16] The use of digital technologies is a key element in ensuring the transparency and effectiveness of tasks implemented by public administration.[17] Despite all its benefits, digitisation also involves the risk of a much greater susceptibility to attacks launched by cybercriminals,[18] who can include both criminal groups operating for profit-oriented or terrorist motives and groups led by foreign states. Such activities are aimed at obtaining information, effecting political or economic destabilisation, or

[12]Suchorzewska (2010), pp. 318–338.

[13]Dawidziak et al. (2009), pp. 55–56.

[14]The term *e-government*, i.e. electronic public administration, describes a system (and, more specifically, an organisational, legal, institutional, and computer system) which makes it possible to handle administrative matters electronically, Ejdys (2018), p. 5.

According to the European Commission, e-government stands for the use of IT tools and systems in order to provide better-quality public services for citizens and enterprises, Glossary of the European Commission https://ec.europa.eu/digital-single-market/en/glossary#letter_e, accessed on 14. September 2020.

[15]Mituś (2013). *Sprawne i skuteczne funkcjonowanie e-administracji przynosi korzyści na trzech poziomach: ludności i podmiotów gospodarczych, organów administracji oraz społeczeństwa i gospodarki jako całości*, cf. Lulkiewicz, *E-administracja (*2013*)*, p. 217.

[16]*A Strategy for Responsible Development (2017)*, the Council of Ministers, Warsaw 2017, p. 226.

[17]See: Śledziewska et al. (2016), pp. 119–130.

[18]According to Interpol, cybercrime is currently a more-profitable activity than drug trafficking (with revenue from such activity in some countries exceeding 1% of GDP), cf. D. Bałut, K. Budek, *Cyberbezpieczeństwo dla przedsiębiorców: Nowa era zagrożeń*, https://marketingibiznes.pl/it/cyberbezpieczenstwo/; accessed on 9 September 2020.

causing social discontent.[19] Notably, any act of disturbing the functioning of cyberspace, whether global or local, affects economic security, the sense of security among citizens, the effective functioning of public-sector institutions, the course of production and service processes, and, in consequence, overall national security.[20]

Therefore, more intensified measures in the field of cybersecurity (i.e. ensuring the protection of the domain of information processing and of interactions within tele-information networks) are indispensable to responding to the growing threat from cybercriminals.[21] It is public administration's duty, in the age of information, to synchronise activities performed by entities operating within various sectors to manage complex networking sites, and to adapt its operational mode so as to be able to explore new technologies, as it is one of the major users of new tools and tele-information technologies, and its functioning is based on the processing of information which forms the principal resource of administration,[22] while information security issues are an element in the laws on national security.[23] For this reason, the public duties (viewed as legal obligations) oriented towards security in cyberspace are a significant aspect of the secure and efficient functioning of the state, and are implemented by way of cooperation between public services and entities in charge of cybersecurity, both at the national (the private sector and NGOs), and international, levels (NATO, the European Union, the UN and supranational associations).[24] Such cooperation plays a major role in the fight against the growing number of incidents being caused by illegal actions in cyberspace, which precipitate financial and image losses.

[19]As e-Government primarily utilises websites as the domain for the exchange of information between administration bodies and citizens, these should meet basic security requirements, i.e. ensure adequate access, integrity and data confidentiality. Otherwise, information might become inaccessible, or might lose its integrity and confidentiality, as a result of impacts originating from various sources, e.g. targeted measures aimed at distributing *malware,* which performs actions on a computer without the consent or knowledge of its user, for the benefit of a third party; disguising oneself as a trustworthy entity, e.g. a renowned institution or person, with the aim of fraudulently obtaining sensitive information (*phishing* and *pharming*); *cross-site scripting,* which involves injecting a malicious code into a given website which takes the user to another website; *SQL Injection,* which involves criminals exploiting various vulnerabilities, e.g., in apps which allow access to personal data to be obtained by unauthorised persons; or *ransomware,* the purpose of which is to take over and encrypt a user's data, and then provide such data to the user on condition that "a ransom" is paid.

[20]*The Cybersecurity Strategy of the Republic of Poland for 2017–2022*, Warsaw 2017, p. 4.

[21]It should be a requirement for public administration to use only the type of electronic equipment which has obtained a special national security certificate. A major element in ensuring a so-called safe supply chain is to assess and certify products, with the establishing of a "national evaluation system" being considered a priority. *Cyberbezpieczeństwo w Polsce: ochrona urządzeń końcowych przed cyberatakami. Analiza sytuacji i rekomendacje działań*, A report prepared by Cyfrowa Polska, Warsaw 2019, pp. 10–11.

[22]Szczepaniuk (2016), p. 26.

[23]Cf. Kamiński (2019b), pp. 57–76; Kamiński (2019a), pp. 28–34.

[24]Bączek (2016), p. 244.

In the Republic of Poland, duties in the field of cyberspace security are implemented by public authorities (legislative, executive, and judicial), and their subsidiary administrative authorities.[25] A significant role of the legislative authorities (the Sejm and the Senate) regarding cybersecurity is to develop legislation and to determine the principal directions of the state's activities.[26] The judicial authorities are entrusted with administering justice in criminal cases, which often involve generally understood national security, and its trans-sectoral domain, i.e. cyberspace security, which is subject to the regulations determining the rules of conduct.[27] The key role in this respect is ascribed to the executive power. The Council of Ministers leading the government's administration, by performing duties to foster the protection of cyberspace, fulfils its constitutional obligations, and bears the main responsibility for ensuring the appropriate level of security for cyberspace and the citizens who function within it.[28]

On 1 August 2018, the President of the Republic of Poland signed the Act on the national cybersecurity system thus implementing within the Polish legal system the Directive of the European Parliament and of the Council (EU) concerning measures for a high common level of security of network and information systems across the Union (Directive 2016/1148).[29] The full implementation of NIS Directive also required adopting two regulations by the Council of Ministers, i.e. on serious incident thresholds,[30] and on a list of essential services and significance thresholds for the consequences of incidents disrupting the provision of essential services.[31]

The national cybersecurity system so established is aimed at ensuring cybersecurity at the national level, including in particular the uninterrupted provision of essential services and digital services, by attaining a sufficiently high level of security of information and communication systems serving the purpose of providing such services, and by ensuring incidents handling.[32]

The system covers operators of essential services[33] (e.g. in the energy, transport, healthcare, and banking sectors), digital service providers, CSIRTs (Computer

[25]Chałubińska-Jentkiewicz (2019), p. 360.

[26]Kitler (2011), pp. 76–77.

[27]Chałubińska-Jentkiewicz (2019). pp. 360–361. See more: Radoniewicz (2016).

[28]Chałubińska-Jentkiewicz (2019), p. 353.

[29]Official Journal EU L 194/1.

[30]The Regulation of the Council of Ministers of 31 October 2018 on serious incidents thresholds (Polish Journal of Laws of 2018, item 2180).

[31]The Regulation of the Council of Ministers of 11 September 2018 on a list of essential services and significance thresholds of the consequences of incidents disrupting the provision of essential services (Polish Journal of Laws of 2018, item 1806).

[32]Article 3 of NCSA.

[33]Operators of essential services, and companies and institutions rendering services in one of the six critical areas, from the point of view of the national economy, i.e. energy, transport, banking, healthcare, potable water supply (and distribution), and the digital infrastructure.

An essential service is considered to be dependent on IT systems. Under Article 17 of the Act on the national cybersecurity system, a digital service provider (DSP) is a legal person or an

Security Incident Response Teams) at the national level, sectoral cybersecurity teams, entities providing services in the field of cybersecurity, responsible bodies in the field of cybersecurity, and single points of contact within the framework of EU cooperation in the field of cybersecurity.

The Act indicates three CSIRTs established at the national level: CSIRT NASK (operating within the Research and Academic Computer Network—the National Research Institute in Warsaw), CSIRT GOV (operating within the Internal Security Agency), and CSIRT MON (operating within the Ministry of Defence). Each CSIRT at the national level has a clearly determined constituency—entities which have a reporting obligation towards that CSIRT, and to which it provides support.

CSIRT MON coordinates the process of handling incidents reported by bodies subordinated to, or supervised by, the Ministry of Defence, including entities whose information and communication systems or networks are included in a consolidated register of facilities, installations, devices, and services forming parts of critical infrastructure, and enterprises of particular economic and defensive significance, for which the Minister of Defence acts as the entity organising and supervising state defence duties.[34]

CSIRT GOV[35] coordinates, on incidents reported by the government administration, units operating within the public finance sector, the National Bank of Poland, Bank Gospodarstwa Krajowego, and operators of critical infrastructure.[36]

CSIRT NASK coordinates on incidents reported by other entities, including operators of essential services (other than operators of critical infrastructure), digital service providers, and local governments.[37] CSIRT NASK can also be referred to as a CERT of last resort, as it is the entity to whom also natural persons (irrespective of their citizenship status or lack of citizenship) and organisational units (irrespective of

computerization unit providing a digital service which does not have legal personality, has its base or management on the territory of Poland, or whose representative runs an computerization unit on the territory of Poland. Small and microenterprises have been excluded from that Act. A list of operators of essential services is maintained by the Minister competent for digital affairs**.** Operators are entered in and removed from the list at the request of a body responsible for cybersecurity; more on the issue: Radoniewicz (2019), p. 55.

[34]https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, accessed on 28 August 2020.

[35]Operating since January 2008 within the Internal Security Agency as CERT.GOV.PL.

[36]In compliance with the Act of 26 April 2007 on Crisis Management, Polish Journal of Laws of 2007 No. 89, item 590, as amended and the Act of 27 August 2009 on public finance, Polish Journal of Laws of 2009 No. 157, item 1240, as amended. CSIRT GOV is mainly entrusted with identifying, preventing, and detecting threats to security, which are important for ensuring the functional continuity of the national tele-information systems utilised by public-administration bodies, or a system of tele-information networks included in a consolidated register of facilities, installations, devices, and services forming parts of the critical infrastructure, as well as tele-information systems of owners and holders of facilities, installations, and devices forming parts of the critical infrastructure, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, accessed on 28 August 2020.

[37]See: *The Deployment of the Baseline Capabilities of National/Governmental CERTs*, ENISA – www.enisa.europa.eu; see also Banasiński and Nowak (2018), pp. 161–162.

their base) can report incidents if no other CSIRTs are considered competent in their case.

Furthermore, CSIRT MIL and CSIRT GOV (in compliance with the Act on Anti-Terrorist Activities and the Act on the Military Counterintelligence Service and the Military Intelligence Service) are competent for handling incidents which constitute acts of terrorism.[38] When it comes to incidents related to national defence, CSIRT MON is always the competent body.

Close cooperation between the CSIRTs established at the national level is the principal assumption of the Act. All the CSIRTs established at the national level are obliged to cooperate both with one another and with competent authorities in the field of cybersecurity, the Minister competent for computerisation, and the Plenipotentiary for Cybersecurity, as well as to ensure a consistent and complete risk management system at the national level, to perform duties related to counteracting cybersecurity threats of a supra-sectoral and cross-border character, and to ensure the coordinated handling of reported incidents (Article 26(1)).

Another major element introduced by the Act on cybersecurity is the possibility of the performing of equipment and software inspections by CSIRTs, with a view to identifying any vulnerabilities which might be used to threaten the integrity, confidentiality, accountability, authenticity, or accessibility of processed data, which might then affect public security or significant national security interests. Based on such inspections, CSIRTs can present recommendations for removing such vulnerabilities in the equipment or software used by entities operating within the national cybersecurity system.[39]

Operators of essential services are also obliged to implement effective security measures, to estimate cybersecurity-related risks, to provide information on major incidents, and to handle such incidents in cooperation with the CSIRTs established at the national level. The entities listed are also obliged to appoint persons responsible for the cybersecurity of the provided services, for incident reporting and handling, and for the dissemination of information on cybersecurity. The national cybersecurity system also includes public administration authorities and telecommunications companies.

In addition, the requirements regarding cybersecurity have been extended to cover digital service providers, i.e. e-commerce platforms, cloud-computing services, and search engines. Given the international nature of these entities, the obligations binding on digital service providers are covered by the regulatory régime harmonised at the EU level (at this point, the Act relates to the relevant Commission Implementing Decision).

[38] Act of 10 June 2016 on Anti-Terrorism (Polish Journal of Laws of 2019, item 796); the Act of 9 June 2006 *on the Military Counterintelligence Service and the Military Intelligence Service*, (Polish Journal of Laws of 2006, No. 104, item 709).

[39] https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, accessed on 28 August 2020.

The national cybersecurity system also includes public entities such as the National Bank of Poland, Bank Gospodarstwa Krajowego, the Office of Technical Inspection, the Polish Air Navigation Services Agency, the Polish Centre for Accreditation, the National Fund for Environmental Protection and Water Management, and regional funds for environmental protection and water management, as well as research institutes and commercial law companies performing public-utility duties.

Under Article 21 of the Act on the national cybersecurity system, each of these entities is obliged to appoint a person in charge of maintaining contacts with entities operating within the national cybersecurity system, as regards public duties dependent on IT systems.

Furthermore, each public entity is obliged to manage incidents within its structures, and to ensure that they are properly handled. Any major incidents must be reported to the competent CSIRT within 24 hours of their being identified (Article 11 (4)). Any decisions made to this end shall require prior consultation with the operator of essential services or the digital service provider which has reported an incident.

CSIRT MON, CSIRT NASK or CSIRT GOV, acting via Single Points of Contact, shall inform other EU Member States of any major incident, as long as it involves two or more EU Member States (Article 29).

The Act has also introduced a formula for Critical Incident Response Teams which act as auxiliary bodies in matters of handling critical incidents, and which comprise the CSIRTs established at the national level and the Government Centre for Security (as a secretariat), to facilitate cooperation with the Government Centre for Crisis Management. Representatives of the competent bodies can also be invited to participate in the work of these Teams.

In compliance with the said Act, information on vulnerabilities and incidents, and the risks of their occurrence, as well as cybersecurity threats, is not subject to the Act on Access to Public Information.[40] Nonetheless, the competent CSIRT MON, CSIRT NASK and CSIRT GOV may publish such information (to the extent necessary) on the websites of the Public Information Bulletin of the Minister of Defence, the Research and Academic Computer Network—National Research Institute, or the Internal Security Agency, as appropriate, if such a transfer of information is likely to contribute to increasing the cybersecurity of the IT systems used by citizens and entrepreneurs, and to ensuring the secure operation of such systems. No published information may, however, violate the provisions on the protection of confidential information or other legally protected secrets, or the provisions on personal-data protection. (Article 35(5)).

Each of the key sectors of the economy is supervised by the competent body in the field of cybersecurity. These include Ministers competent for individual

[40]Act of 6 September 2001 on access to public information (consolidated text Polish Journal of Laws of 2019, item 1429, as amended).

administration departments,[41] who, by way of memoranda of understanding, can entrust some of their duties to subsidiary or supervised units. In practice this means that sectoral regulators (if any) may fulfil such functions instead of the competent Ministers.

The competent body in the field of cybersecurity is in charge of analysing entities operating in a given sector, and issuing decisions on the recognition of operators of essential services. In addition, it prepares recommendations on actions to strengthen the cybersecurity of that sector, and is in charge of calling on operators to remove any vulnerabilities which could lead, or could have led, to serious incidents, conducting inspections of operators of essential services, cooperating with other EU Member States via Single Points of Contact, participating in training, and processing personal data necessary for its duties to be fulfilled.[42]

In justified cases, the authorities competent for cybersecurity and the Single Point of Contact cooperate with law enforcement authorities and the entity competent for personal data protection (Article 42(7)).

The civil aspects of the cybersecurity of the Republic of Poland remain within the remit of the Minister competent for computerisation. That Minister, in cooperation with the Plenipotentiary for Cybersecurity, and other Ministers, is responsible, *inter alia*, for developing the Cybersecurity Strategy,[43] implementing information policies regarding the national cybersecurity system, fulfilling reporting obligations towards EU institutions, and launching, as of 1 January 2021, an information and communication system enabling automated incident reporting and handling, ICT

[41]Under Article 41 of the NCSA, the competent authorities in the field of cybersecurity are as follows: for the energy sector—the Minister competent for energy; for the transport sector, excluding the water-transport subsector—the Minister competent for transport; for the water-transport subsector—the Minister competent for the maritime economy and the Minister competent for inland shipping; for the banking sector and the financial-market infrastructure—the Polish Financial Supervision Authority; for the healthcare sector—the Minister competent for health; and for the potable-water supply and distribution sector—the Minister competent for water management. In addition. for the digital infrastructure sector and digital service providers—the Minister competent for computerisation; and for healthcare, digital infrastructure and digital service providers (to the extent as defined in the Act)—the Minister of Defence (entities subordinated to the Minister of Defence and companies of particular economic and defense significance).

[42]The Act on the National Cybersecurity System in: https://cyberpolicy.nask.pl/ustawa-o-krajowym-systemie-cyberbezpieczenstwa, accessed on 10 September 2020.

[43]The Security Strategy lays down the strategic objectives, and the appropriate political and regulatory measures which make it possible to attain (and maintain) a high level of cybersecurity. The Security Strategy also specifies the priorities, the entities engaged in its implementation, and the activities regarding educational and informational programmes, as well as research-and-development plans. It is adopted by way of a Resolution by the Council of Ministers. On 22 October 2019, the Council of Ministers adopted a Resolution on the Cybersecurity Strategy of the Republic of Poland for 2017-2022 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037). The document has been in force since 31 October 2019, replacing *the National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022*. The Minister competent for computerisation, in cooperation with other members of the Council of Ministers, is responsible for implementing the provisions of the said document, and for presenting, by 30 March of each year, information on the implementation of the Strategy.

risk estimation, and warnings about cybersecurity threats, recommending fields of cooperation with the private sector, implementing information measures regarding good practices, educational programmes, campaigns and training courses aimed at expanding knowledge on and raising awareness of cybersecurity. The Minister also runs the Single Point of Contact, which is responsible for cooperating with the European Commission and submitting annual reports; it also cooperates with other Member States in the field of cybersecurity, and coordinates cooperation between competent national authorities (Articles 45–50).

The major duties of the Minister of Defence include facilitating international cooperation between the Armed Forces of the Republic of Poland and the responsible bodies of NATO, the EU, and other international organisations, in the field of defence, and, more specifically, cybersecurity. The Minister of Defence is also responsible for guaranteeing the capabilities of the Armed Forces of the Republic of Poland, within the national, alliance, and coalition systems; for conducting military activities in the event of a cybersecurity threat's triggering the need for defence measures; for developing the abilities of the Armed Forces of the Republic of Poland of ensuring cybersecurity by launching specialised training initiatives; for acquiring and developing tools for building capabilities for ensuring cybersecurity in the Armed Forces of the Republic of Poland; for assessing the impact of incidents on the national defence system; and for managing activities related to incident handling during martial law (Articles 51–52).

As the cybersecurity issues are horizontal, i.e. they involve several Ministries and governmental agencies, the Act envisaged establishing the College for Cybersecurity and the Plenipotentiary for Cybersecurity, for the purpose of coordinating related policies on the national scale. The Plenipotentiary is to pursue international cooperation, to support the scientific research and development of technologies in the field of cybersecurity, to take measures to raise the public's awareness of cybersecurity threats, and to promote the safe use of the Internet. That person is also entrusted with analysing and assessing the functioning of the national cybersecurity system, supervising the process of risk management within the national cybersecurity system, issuing opinions on governmental documents, including draft legal Acts appropriate for the implementation of cybersecurity duties, and issuing recommendations on the use if IT tools or software at the request of the responsible CSIRT.

The Plenipotentiary is appointed and dismissed by the President of the Council of Ministers from among secretaries or under-secretaries of state, and is accountable to the Council of Ministers (Articles 60–63).

The College for Cybersecurity is an opinion-making and advisory body to the Council of Ministers regarding cybersecurity issues and activities conducted in this field by CSIRTs, the Ministry of Defence, CSIRT NASK, CSIRT GOV, sectoral cybersecurity teams, and authorities competent for cybersecurity (Article 64). The Committee is led by the President of the Council of Ministers, and is composed of the Minister competent for internal affairs, the Minister competent for computerisation, the Minister of Defence, the Minister competent for foreign affairs, the Chancellery of the President of the Council of Ministers, the Head of the National Security Bureau, and the Minister competent for coordinating the activities of special

forces. Committee meetings are also attended by the Director of the Government Centre for Security, the Head or Deputy Head of the Internal Security Agency, the Head or Deputy Head of the Military Counterintelligence Service, and the Director of the Research and Academic Computer Network—National Research Institute (Article 66). The scope of responsibilities of the College for Cybersecurity was outlined in Article 65 of the Act.[44]

The implementation of the National Cybersecurity System Act is a challenge both for the administration and private sectors. Constructing an efficiently functioning system in various sectors is another huge challenge arising from that Act (as it entails establishing sectoral cybersecurity teams and amending sector-specific provisions). The competent bodies must, in the first place, develop expertise regarding supervision over cybersecurity issues. The incident-reporting obligation is a major change for the private sector, which also becomes challenging for the administration when it comes to developing specific tools[45]—e.g. an information and communication system—which, in principle, is to support the national cybersecurity system. The practical implementation of these activities will be crucial for the safe functioning of the state's power structures.

The rapid development of the Internet, coupled with ICT expansion, have caused, *inter alia*, the globalisation of economic, social and political phenomena.

The functioning of the state and the implementation of its constitutional duties increasingly depends on the development of modern technologies, the information society, and the uninterrupted functioning of cyberspace. The last of these, in turn, is largely dependent on the security of the ICT infrastructure which facilitates the use of cyberspace, and the information resources and services which function within it. Continuous education and raising the awareness of public servants regarding issues related to cyberspace security, and in particular appropriate and effective protection, should be a major responsibility of the state. Special attention should be paid to educating those in charge of public procurement in offices and public institutions. Ultimately, entities ordering equipment and services which can potentially be threatened by cyber attacks should choose such solutions which guarantee digital safety.

The results of inspections regarding the management of information security in local government units, conducted by the Supreme Chamber of Control in 2018, showed that awareness among persons fulfilling major functions in the National Cybersecurity System regarding the importance of information security issues was insufficient. The shortage of both financial resources to implement major undertakings, and of information security experts, was also brought to light, these being two major aspects which the national authorities should seek to address.

Security in cyberspace is the newest, and currently the most demanding, field of national security, which combines defence and protection, civil and military, and

[44]See also: Brzostek (2019), pp. 146–147.

[45]This is quite a novelty in the Polish legal order, as previously—except for the communications sector—there was no obligation to report incidents.

also public and private, aspects. Ensuring cybersecurity in Poland, and constructing a system resistant to threats, constitute an ongoing process, which, as should be noted, is becoming more deliberate and planned, despite the emerging challenges and difficulties which were not known before.

References

Bączek P (2016) Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruń
Bałut D, Budek K. Cyberbezpieczeństwo dla przedsiębiorców: Nowa era zagrożeń. https://marketingibiznes.pl/it/cyberbezpieczenstwo/. Accessed 10 Oct 2020
Banasiński C Nowak W (2018) Europejski i krajowy system cyberbezpieczeństwa in: Cyberbezpieczeństwo. Zarys wykładu, Warsaw
Borkowski M (2013) Cyberprzestrzeń a bezpieczeństwo jednostki, Warsaw
Brzostek A (2019) Polityka ochrony cyberprzestrzeni administracji publicznej na przykładzie organów administracji rządowej wskazanych w ustawie o Krajowym Systemie Cyberbezpieczeń. In: Kitler W, Chałubińska-Jentkiewicz K, Badźmirowska-Masłowska K (eds) System bezpieczeństwa w Cyberprzestrzeni RP. Warszawa
Chałubińska-Jentkiewicz K (2019) Cyberodpowiedzialność, Toruń
Dawidziak P Łęcki B Stolarski M (2009) Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa. In: Madej M, Terlikowski. Bezpieczeństwo M (eds) Teleinformatyczne państwa, Warsaw
Dubiel AJ (2018) System Bezpieczeństwa Narodowego. https://mil.link/en/wp-content/uploads/2018/01/SBN.pdf. Accessed 10 Oct 2020
Ejdys J (2018) Zaufanie do technologii w e-administracji. Białystok
Gołębiowska A (2015) Local Government in the Constitution of the Republic of Poland of 1997. Ius Novum 2(29)
Kamiński MA (2019a) Military law in the Republic of Poland. Safety Defence 5
Kamiński MA (2019b) Prawo bezpieczeństwa narodowego. Wiedza Obronna 3(268)
Kitler W (2011) Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system, Warsaw
Kuciński J (2008) Nauka o państwie i prawie, Warsaw
Lulkiewicz E, E-administracja (2013) Korzyści i zagrożenia. In: Stanisławski T, Przywora B, Jurek Ł (eds) E-administracja. Szanse i zagrożenia, Lublin
Mituś A (2013) E-administracja: korzyści i zagrożenia. In: Suwaj JP, Zimmerman J (eds) Wpływ przemian cywilizacyjnych na prawo administracyjne i administrację publiczną, Lex/el 2013
Radoniewicz F (2016) Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warsaw
Radoniewicz F (2019) Article 4 (The scope of application). In: Kitler W, Taczkowska-Olszewska J, Radoniewicz F (eds) The Act on the national cybersecurity system. Commentary. Warsaw
Śledziewska K Levai A Zięba D (2016) Use of e-Government in Poland in comparison to other European Union Member States. Information Systems in Management 1(5)
Suchorzewska A (2010) Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem, Warsaw
Szczepaniuk E (2016) Bezpieczeństwo struktur administracji w warunkach zagrożeń cyberprzestrzenią państwa, Warsaw

Marzena Toumi dr hab., associate professor at the War Studies University in Warsaw; advocate; a graduate of Faculty of Law, Canon Law and Administration at the John Paul II Catholic University of Lublin and a graduate of the 4th edition of the Annual Diplomatic Program of the Academy of Foreign Affairs—House of Diplomacy. Director of the Institute of Law and Head of the Department of History and Theory of Law at the War Studies University in Warsaw. Vice President of the Association of the Center for Comparative Studies. Author of monographs, textbooks and publications, including in the field of history of law as well as constitutional and legal systems of modern countries.