The Cybersecurity Strategy of the Republic of Poland

Waldemar Kitler

Abstract Directive 2016/1148 obliged each Member State to have a national strategy in the field of network and information system security, defining strategic goals and specific policy actions to be implemented. The adoption of the “Cybersecurity Strategy of the Republic of Poland” is also a requirement to implement the provision of Article 68 of the Act of 5 July 2018 on the National Cybersecurity System.

The strategy for the years 2019–2024, which defines targets in the field of cybersecurity, set the main goal, i.e. increasing the level of resilience to cyber threats and increasing the level of information protection in the public, military, and private sectors and promoting knowledge and good practices enabling citizens to better protect their information.

As part of the activities planned in the Strategy until 2024, the Government of the Republic of Poland will systematically strengthen and develop the National Cybersecurity System. The activities include systemic organisational, operational, technological, and legal solutions, creating social attitudes and conducting scientific research in order to ensure compliance with high cybersecurity standards in the area of software, devices and digital services. Government activities will be undertaken with respect for the rights and freedoms of citizens and by building trust between individual market sectors and public administration.

W. Kitler (✉)

Faculty of National Defence, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: w.kitler@akademia.mil.pl

© The Author(s) 2022

K. Chałubińska-Jentkiewicz et al. (eds.), *Cybersecurity in Poland*,
https://doi.org/10.1007/978-3-030-78551-2_9

1 Introduction

The adoption of the NIS Directive¹ by the European Parliament and the Council (EU) obligated Member States to develop their own national strategies on the security of network and information systems. Under Article 7(1) of the NIS Directive,

Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of security of network and information systems, and covering at least the sectors referred to in Annex 2 and the services referred to in Annex 3.

In consequence, on 27 April 2017 the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022² was adopted by way of Resolution No. 52/2017 of the Council of Ministers, along with the accompanying document entitled “The Action Plan for Implementing the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022.” It is also worth noting that in the same year the Minister competent for Digital Affairs adopted a document entitled “The Cybersecurity Strategy of the Republic of Poland for 2017–2022.” All the above-mentioned documents envisaged the continuation of measures implemented by the government administration with the aim of improving the level of security in the cyberspace of the Republic of Poland, as well as the document entitled “The Governmental Cyberspace Protection Programme of the Republic of Poland for 2009–2011 – assumptions,” discussed on 9 March 2009 by the Standing Committee of the Council of Ministers, and the Cyberspace Protection Policy of the Republic of Poland adopted by the Government in 2013.³ It should be stressed at this point that, before the entry into force of the Cybersecurity Strategy of the Republic of Poland for 2019–2024, the role of a similar-stature document had been played by the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022, adopted by way of Resolution No. 52/2017 of the Council of Ministers of 27 April 2017 on the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022.

Two years after the adoption of the NIS Directive, the Polish Sejm passed the Act of 5 July 2018 on the National Cybersecurity System,⁴ following which, under

¹Directive 2016/1148 of the European Parliament, and of the Council (EU), of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (OJ EU 2016 L 194/1).

²Resolution No. 52/2017 of the Council of Ministers of 27 April 2017 on the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022 (KPRM), RM-111-52-17.

³Resolution No. 111/2013 of the Council of Ministers of 25 June 2013 on the Cyberspace Protection Policy of the Republic of Poland, KPRM, RM-111-103-13.

⁴Polish Journal of Laws of 2018, item 1560 as amended.

Article 68 thereof, the legislator developed formal grounds for the adoption of the Cybersecurity Strategy of the Republic of Poland by the Council of Ministers.⁵

2 The Cybersecurity Strategy vs. Normative Acts and Strategic Documents

The provisions of the Constitution of the Republic of Poland stipulate that the Council of Ministers shall conduct the internal affairs and foreign policy of the Republic of Poland (Article 146(1)), and to the extent, and in accordance with, the principles specified by the Constitution and Acts, it shall, in particular, guarantee the implementation of Acts (Article 146(4)(1)); safeguard the internal security of the state and public order (Article 146(4)(7)); and ensure the external security of the state (Article 146(4)(8)). The national security of the Republic of Poland, in both the subjective and objective scopes, is dependent on the uninterrupted functioning of cyberspace, to the same extent as its very existence and development. In consequence, ensuring the resilience of information systems against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems, is among the major challenges faced by the Polish administration, in particular at the central level.

Cybersecurity, including the national cybersecurity system which is being constructed to secure the accomplishment of the set objectives, is now a key sphere of national security, in its both internal and external dimensions. In addition, considering the increasingly blurred boundaries between these two dimensions, the strategy must take into account any actions, regardless of state borders, which violate the confidentiality, integrity, availability, and authenticity of the processed data or related services provided through network and information systems.

The strategy, by outlining the mode of accomplishing the security policy objectives regarding cyberspace, determines the directions of the state's activities and the method of fulfilling its potential. However, certain doubts can arise in connection with its normative status, despite its being developed and adopted under the NCSA.

The draft version of that document, which, at the request of the Minister competent for computerisation, was developed in cooperation with the Government Plenipotentiary for Cybersecurity⁶ other Ministers and the appropriate managers of central governmental offices (see Article 70 of the NCSA), is to be adopted by the Council of Ministers by way of a Resolution. In compliance with Article 68 of the

⁵The name adopted in the said Act (see Article 45(1)(1)). It was also used in the title of the draft Act in *"The list of the legislative and programme work of the Council of Ministers,"* reading as *"A draft Act of the Council of Ministers on the Cybersecurity Strategy of the Republic of Poland,"* draft No. ID210. Eventually, that name was also used in Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024 (The Official Gazette of the Government of the Republic of Poland of 30 October 2019, item 1037).

⁶Hereinafter referred to as "the Plenipotentiary",

NCSA, the strategy is to be adopted by the Council of Ministers under an internal legal act, i.e. by way of a Resolution. However, the Polish legislators did not adopt a legal definition of the term *cybersecurity strategy* (of the Republic of Poland), but it indicated, by way of an Act, the elements which this document should feature (Article 69(2) of the NCSA) and determined its legal form. Among other documents related to national security of strategic importance, this is one of the few examples of making a strategy a state-level document. In the vast majority of cases, the legislator merely authorised the responsible bodies to develop, announce, and adopt specific strategies. The latter situation involved the National Security Strategies of the Republic of Poland of 2007 and 2014, for which the legal grounds were provided by Article 4a(1)(1) and Article 6(1)(1) of the Act of 21 November 1967 on the Universal Duty to Defend the Republic of Poland,⁷ the Strategy for the Development of the National Security System of the Republic of Poland 2022, and the Strategy for Responsible Development by 2020 (including a 2030 perspective), both adopted by way of Resolutions of the Council of Ministers under Articles 9 and 12a of the Act of 6 December 2006 on the Principles of Conducting the Development Policy.⁸ As a result, the executive authorities, and in particular the Government authorities, used to have a decisive voice when it came to the structure of the strategic documents of this stature. This time, however, the legislator determined the framework of the substantive structure of the Strategy, although this decision was somewhat imposed to ensure compliance with the requirements laid down in Article 7(1) of the NIS Directive.

In connection with the above, the legal effect of the directives (which have the character of programmatic norms) included in the Strategy can be questioned, *inter alia*, due to the fact that their provisions regarding purpose and content might not be directly binding on public authorities, or other entities in the national cybersecurity system, which, in compliance with the Constitution of the Republic of Poland, operate on the basis of and within the law. Resolutions and other internal legal acts form a separate set of normative acts, and govern only the relationships between the organisational units forming part of the apparatus supervised by the body which issues a given Resolution or internal legal act. Resolutions of the Council of Ministers may be addressed to subordinate units, and, thus, any strategies adopted on that basis bind only those subordinate units (Article 93(1) of the Constitution of the Republic of Poland), and they may not serve as the basis for decisions taken in respect of citizens, legal persons, or other entities (Article 93(2) thereof). Given the substantive content of the Strategy (Article 69 of the NCSA) and some elements included in the national cybersecurity system (Article 4), the above doubts can be justified. This concerns in particular the National Bank of Poland, Bank

⁷Act of 21 November 1967 on the Universal Duty to Defend the Republic of Poland, consolidated text, Polish Journal of Laws of 2019, item 1541, as amended.

⁸Act of 6 December 2006 on the Principles of Conducting the Development Policy, Polish Journal of Laws of 2009 No. 84, item 712, as amended.

Gospodarstwa Krajowego, companies and partnerships, and some entities performing cybersecurity services.

It can be concluded, therefore, that the national cybersecurity system includes some entities which cannot be subject to the provisions of the Strategy. Under Article 4 of the NCSA, the national cybersecurity system consists of: operators of essential services—digital service providers; CSIRT MON; CSIRT NASK; CSIRT GOV; sectoral cybersecurity teams; units operating within the public-finance sector referred to in Articles 9(1-6), (8), (9), (11) and (12) of the Act on Public Finance; research institutes; 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; companies and partnerships performing public-utility duties within the meaning of Article 1(2) of the Act on Municipal Services; entities providing services in the field of cybersecurity; bodies in charge of cybersecurity;⁹ the Single Point of Contact for cybersecurity;¹⁰ the Government Plenipotentiary for Cybersecurity; and the College for Cybersecurity.¹¹

It can be concluded that, given the status of the Strategy, it can have a direct impact on government administration authorities, and, given its legal status in relation to generally applicable law, its impact on other public authorities, entrepreneurs, and citizens is only indirect.

It should also be stressed that several government administration bodies were appointed by the legislator for the purpose of developing, and then adopting, the Strategy. These included the Minister competent for computerisation, who was obliged to cooperate with the Plenipotentiary, other Ministers, and the appropriate managers of central offices (in developing the draft version of the Strategy), and the Council of Ministers (passing a Resolution on adopting the Strategy). The mere fact of finalising the draft version of the Strategy reflects the good will and agreement of the authorised bodies as to its content, by which they express their standpoint on the

⁹The competent bodies 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, excluding the entities referred to in Article 26(5)—the Minister competent for health; for the healthcare sector including the entities referred to in Article 26(5)—the Minister of National Defence; for the potable-water supply and distribution sector—the Minister competent for water management; for the digital-infrastructure sector, excluding the entities referred to in Article 26(5)—the Minister competent for computerisation; for the digital infrastructure sector, including the entities referred to in Article 26(5)—the Minister of National Defence; for digital service providers, excluding the entities referred to in Article 26(5)—the Minister competent for computerisation; and for digital service providers, including the entities referred to in Article 26(5)—the Minister of National Defence (Article 41 of the NCSA).

¹⁰Hereinafter referred to as “the Single Point of Contact”.

¹¹Hereinafter referred to as “the College”.

subject matter. The ultimate Act, for it to be adopted, engages the whole Council of Ministers, and requires a consensus to be reached by way of discussions attended by the majority of the Council of Ministers at Council meetings (§ 15(1) and (2) of the Resolution of the Council of Ministers of 29 October 2013 *Internal Working Regulations of the Council of Ministers*).¹² The Resolution of the Council of Ministers becomes binding on all its members who “[...] shall be collectively responsible to the Sejm for the activities of the Council of Ministers” (Article 157 (1) of the Constitution of the Republic of Poland).

Summing up, it can be stated that, in view of the current legal status, the Strategy adopted by the Council of Ministers can be applicable across the Government’s administration, but without covering other public entities or institutions, local government authorities, businesses not owned by the state, or non-governmental organisations.

3 The Vision, Main Goal, and Specific Objectives of the Strategy

In compliance with Article 60(1) of the NCSA,

The Strategy determines the strategic objectives, and the appropriate political and regulatory measures, aimed at attaining and maintaining a high level of cybersecurity. The Strategy shall cover the sectors referred to in Annex 1 hereto, and the digital services and the public entities referred to in Article 4(7)-(15).

The Council of Ministers, in adopting the Resolution on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, strengthened the strategic objectives by introducing the heading “Vision, main goal, specific objectives.”

The vision assumes that

The efficient and safe operation of information systems and means of electronic communication are related to the successful growth of the Republic of Poland, the increasing wealth and effectiveness of the economy, and the performance of its institutions and entities, including the social activities and everyday functioning of individual members of society. Therefore, as part of the actions planned in the Cybersecurity Strategy by 2024, the Government shall systematically enhance and develop the national cybersecurity system. The said actions include systemic organisational, operational, technological, and legal measures, as well as the shaping of social attitudes, and conducting research and development projects, to ensure the achievement of high cybersecurity standards of software, hardware, and digital services. The Government shall take these actions by building confidence between the private sector and the public administration, while respecting the rights and freedoms of the citizens—(Point 4.1 of the Strategy).

¹²The Resolution of the Council of Ministers of 29 October 2013 *Internal Working Regulations of the Council of Ministers*. The Official Gazette of the Government of the Republic of Poland of 2016, item 1006, as amended.

In Article 69(1) of the NCSA, the legislator stipulated that the Strategy should determine the strategic objectives and the appropriate political and regulatory measures, aimed at attaining and maintaining a high level of cybersecurity. This resulted from the provisions of the NIS Directive which, in the definitions section, *stipulated*

the ‘national strategy on the security of network and information systems’ entails a framework providing strategic objectives and priorities on the security of network and information systems at the national level—(Article 4(3)).

Furthermore,

Each Member State shall adopt a national strategy on the security of network and information systems, defining the strategic objectives and the appropriate policy, and regulatory measures, with a view to achieving and maintaining a high level of security of network and information systems, and covering at least the sectors referred to in Annex 2 and the services referred to in Annex 3. (Article 7(1), sentence 1).

Such an approach is consistent with the prevailing view of the essence of the strategy as such, which J. Penc defined as a concept of

[...] systemic action (an action plan) which involves formulating a set of long-term business objectives, and modifying these objectives, depending on changes occurring in the business environment, and determining the resources and means for these objectives to be fulfilled (...).

A similar way of reasoning regarding the Strategy was adopted when implementing the national development policy, in which it was defined as “[...] a process of creating and implementing a long-term plan, attaining a certain standing, and securing a relatively permanent operational model,” and the strategy of an organisation as “a set of non-concurrent operating modes, adjusted to its potential and circumstances, enabling its long-term objectives to be fulfilled.” In consequence, developing a strategy implies

[...] selecting the field of operation in which the organisation is seeking to establish its presence, and determining the means necessary for its survival and development, i.e. for gaining a stronger competitive edge within the sectors, and on the markets, in which it is pursuing its activities.

The state is to ensure the national existence and development conditions which are free from disruptions (and, in particular, threats), which fact was reflected in Article 5 of the Constitution of the Republic of Poland, reading

The Republic of Poland shall safeguard the independence and integrity of its territory, and ensure the freedoms and rights of persons and citizens, the security of its citizens, safeguard the national heritage, and shall ensure the protection of the natural environment, pursuant to the principles of sustainable development.

Also, numerous legislative acts contain the standards defined by the legislators in laying down the duties of public authorities, and other public entities and institutions, businesses, social organisations, and citizens, regarding the state’s (or national) security. All these regulations involve, to a large extent, the fulfilment of the state’s external and internal functions, including, in particular, law-enforcement, organisational, executive, regulatory and planning functions.

In determining the strategic objectives, the Council of Ministers lays down the cybersecurity goals which are expected to be attained in the future. These correspond to the anticipated operational outcomes expressed through programmatic norms and directives which cannot be made into legal norms. For this reason, the Strategy may be neither an Act nor a regulation, as its provisions govern a certain operational programme of public administration, within the framework of the national cybersecurity strategy, but they are rather unspecific and imprecise, while their legal enforcement would be hindered.

An illustration of the determining of strategic objectives is provided in Article 3 of the NCSA, reading

The national cybersecurity system is aimed at ensuring cybersecurity at the national level, including the uninterrupted provision of essential services and digital services, by attaining a sufficient level of security of information systems serving the purpose of providing such services, and by ensuring incident handling.

Notwithstanding the foregoing, one should note that, in determining the strategic objectives, the Council of Ministers is driven by substantive factors and the principles of defining the organisation's goals. In the first case, this refers to following the provisions of both the NIS Directive and the NCSA and the EU Internal Security Strategy and national strategies (regarding security and development).

The Strategy for 2019–2024, determining the cybersecurity objectives, also contains the main goal, i.e.

Increasing the level of resilience to cyber threats and the protection of information in the public, military and private sectors, as well as promoting knowledge and good practices to enable the public to better protect information.

The main goal is followed by five specific objectives.¹³

- Specific objective 1—The development of the national cybersecurity system, (including the implementation and evaluation of the functioning of the provisions regarding the national cybersecurity system; enhancing the efficiency of the functioning of the national cybersecurity system; the development of an information sharing system for the purpose of national security management; enhancing the cybersecurity of essential and digital services and critical infrastructure; the development and implementation of a risk assessment methodology at the national level; and increasing the capacity to counteract cybercrime, including cyber espionage and incidents of a terrorist nature).
- Specific objective 2—Increasing the resilience level of information systems of the public administration and private sectors, and building the capacity to effectively prevent and respond to incidents (including the development and implementation of National Cybersecurity Standards, and the dissemination of good practices and recommendations; supply chain security; and security tests and audits).

¹³See The Cybersecurity Strategy of the Republic of Poland for 2017-2022, Appendix to Resolution No. 125 of the Council of Ministers of 22 October 2019 Official Gazette of the Government of the Republic of Poland of 2019, item 1037.

- Specific objective 3—Increasing the national capacity in the sphere of cybersecurity technology (including the development of industrial and technological resources for the purposes of cybersecurity; focus on developing public-private cooperation; stimulating research and development in the field of cybersecurity; and building the capacity to perform a full spectrum of military operations in cyberspace);
- Specific objective 4—Enhancing public awareness and skills in the field of cybersecurity (including increasing the expertise of the staff of entities applicable to ensuring the cybersecurity of the Republic of Poland; creating conditions for the safe use of cyberspace by citizens; and developing public awareness towards the safe use of cyberspace);
- Specific objective 5—Establishing a strong international position of the Republic of Poland in the sphere of cybersecurity (including: active international cooperation at the strategic and political levels; and active international cooperation at the operational and technical levels).

4 The Means for Fulfilling the Strategy's Objectives and the Entities Involved in Its Implementation

The legislators obligated the Council of Ministers to determine the means for achieving the Strategy objectives. These should, in principle, ensure the level of security of network and information systems commensurate with the risk presented, by preventing and minimising the impact of incidents on the security of the network and information systems which are used for the provision of essential services. These will be technical and organisational measures, accompanied by normative (legal) and administrative measures ensuring that the authorised bodies, the operators of essential services, and providers of essential services, are vested with the necessary rights. These are contained, to a greater or lesser extent, in the specific objectives.

The means for accomplishing the objectives are determined both via programmatic norms and technical directives, as the former are intended to set the goals to be fulfilled, and the latter specify various entities, priorities, means, and other activities, in accordance with Article 69(2) of the NCSA. This aspect of the strategy is reflected in the current achievements and traditions related to developing strategic documents, and in the content of the National Framework of Cybersecurity Policy of the Republic of Poland¹⁴ for 2017–2022¹⁵ adopted by way of Resolution No. 52/2017 of the Council of Ministers of 27 April 2017.

If we assume that policy measures are any activities undertaken by public authorities with a view to attaining the set objectives, then attention should be paid to the fact that, in the reference Strategy, the Council of Ministers designates, in

¹⁴hereinafter “the National Framework”.

¹⁵KPRM/RM-111-52-17.

varying degrees, activities at the international and national levels (economic, military, educational, scientific and technical, normative, and special), in compliance with the NCSA.

In turn, regulatory measures are implemented to ensure compliance with both the NIS Directive and the NCSA, in order to attain and maintain a high level of cybersecurity. Therefore, the regulations should seek, under the NCSA, *inter alia*, to ensure the consistency of the developed cybersecurity system as regards supervision over financial markets, the adjustment of the banking sector's and the financial markets' infrastructure, the conclusion of agreements for the provision of essential ICT services, and the security of network and information systems of operators of essential services and digital service providers.

Prior to entry into force of the NIS Directive and the NCSA, the national regulatory framework for electronic communications networks and services had been defined in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).¹⁶ The Directive lays down a common legal framework for the provision of electronic communications services, electronic communications networks, and associated facilities and services. It also lays down the tasks of national regulatory authorities, and establishes a set of procedures to ensure the harmonised application of the regulatory framework throughout the Community (Article 1(1) of Directive 2002/21/EC).

Similar to political measures, regulatory measures should also ensure the attaining and maintaining of a high level of cybersecurity.

Under Article 69(1), the Strategy shall cover the sectors referred to in Annex 1 hereto, and the digital services and the public entities referred to in Article 4(7)-(15) (Official Journal EU L 194/1 of 19.07.2016, p 1). Considering that the NIS Directive lays down the obligations serving the purpose of ensuring the cybersecurity of information systems in the services sectors which are essential for the maintenance of social and economic activities, the legislators, by performing minor substantive modifications, indicated (Annex 1 to the NCSA) the sectors, subsectors and types of entities in respect of which the body in charge of cybersecurity has issued a decision on recognising an operator of essential services (see Article 5(2)). These are energy, transport, banking, financial market infrastructure, healthcare, water supply and digital infrastructure. The sectors, subsectors, and types of entities providing essential services were defined in further detail, together with significance thresholds of the consequences of incidents disrupting the provision of essential services, in an Annex to the Regulation of the Council of Ministers of 11 September 2018, a list of essential services and significance thresholds of the

¹⁶Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), OJ EC 2002 L 108/33 (hereinafter: Directive 2002/21/EC).

consequences of incidents disrupting the provision of essential services.¹⁷ The Regulation, within its scope of application, serves the purpose of implementing the NIS Directive.

The entities involved in the Strategy implementation, which need to be indicated in its provisions, are in fact listed in the Act. These are the entities which, under Article 4 of the NCSA, comprised the national cybersecurity system, i.e. the operators of essential services listed in Annex 1 to the said Act; digital service providers (see the commentary to Chapter 4); CSIRT MON; CSIRT NASK; CSIRT GOV; sectoral cybersecurity teams; units operating within the public finance sector referred to in Article 9(1-6), (8), (9), (11) and (12) of the Act on Public Finance; research institutes; 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; companies and partnerships performing public utility duties within the meaning of Article 1(2) of the Act of 20 December 1996 on Municipal Services; entities providing services in the field of cybersecurity; competent authorities for cybersecurity; the Single Point of Contact; the Government Plenipotentiary for Cybersecurity; and the College for Cybersecurity.

5 The Means for Readiness, Response and Restoration

The specification of the means for readiness, response, and restoration, including the principles of public-private cooperation, constitutes another element of the Strategy. Their description was also, though to a minor extent, included in the content of the specific objectives.

The entire set of the means for readiness, response, and restoration had been previously implemented in the field of the state's defensive readiness and alert levels, as well as in crisis management. However, systemic cybersecurity solutions were lacking. In the statement of grounds for the Act, it was stated that Poland had no "[...] statutory provisions determining the detailed scope of the competences of specific bodies in the field of cybersecurity, in relation to sectors defined in the Directive¹⁸". Prior to adopting the Act, the National Framework envisaged the determining of the scope of responsibilities, obligations, and rights of the system participants, and the ways of interacting with and between other system participants. More specifically, they assumed the defining of the competences of the appropriate

¹⁷ Regulation of the Council of Ministers of 11 September 2018, 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 r., item. 1806.

¹⁸ Statement of grounds, p. 11, <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505> Accessed on 10.10.2020.

bodies in charge of supervising information systems in the sectors within which essential services and digital services are provided.¹⁹ Nonetheless, one should bear in mind that the National Framework was not a national product, but its development was based on the draft version, and then the final version, of the NIS Directive. The Act merely sanctioned, at the appropriate level, the provisions of the document adopted by the Council of Ministers, by way of a Resolution.

Despite the benefits of adopting the new Act and determining the means for readiness, response, and restoration, the need to allocate competence between several legal administrations, i.e. the state's defensive readiness, crisis management, and the three states of emergency (natural disaster, the state of exception, and martial law), must be borne in mind.

Ensuring cyberspace security requires concerted efforts from the private and public sectors. Building an effective public-private partnership system based on trust and shared responsibility can constitute a major security pillar in cyberspace.

The public administration shall, at the same time, improve its potential to advise market sectors in the field of ICT security. The government shall also actively engage in the existing and emerging forms of European public-private cooperation, and thus promote Polish business at the international level.²⁰

As stressed by M. Ganczar

The EU legislators have noted that most of the network and information systems are utilised by private entities; therefore, it has been continually implementing the previous assumptions regarding the creation of a contractual public-private partnership for cybersecurity.²¹

The author also stressed that the operators and providers of essential services should be encouraged to create their own and informal cooperation mechanisms in this field.

6 Risk Assessment

The risk-assessment approach constitutes a major element of the Strategy, which results from the requirements laid down in the EU directive and the national Act. As stipulated in the NIS Directive, "Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents, and to mitigate their impact" (recital 46, sentence 1 of the NIS Directive). It should also be stressed that, from the point of view of the EU legislators,

In practice, the degree of risk for operators of essential services, which are often essential for the maintenance of critical societal and economic activities, is higher than for digital service providers. Therefore, the security requirements for digital service providers should be less

¹⁹Ibidem.

²⁰The National Framework..., Point 7.2.

²¹M. Ganczar (2017), p. 87.

stringent. Digital service providers should remain free to take measures they consider appropriate to manage the risks posed to the security of their network and information systems. Because of their cross-border nature, digital service providers should be subject to a more harmonised approach at the Union level. Implementing acts should facilitate the specification and implementation of such measures—(recital 49).

From the legislators' point of view, risk is "[...] a combination of the likelihood of the occurrence of an adverse event and its consequences," whereas risk management means "[...] coordinated activities in the field of cybersecurity management in relation to the estimated risk" (Article 2(12) and Article 2(19) of the NCSA, respectively). Such a risk interpretation is characteristic of almost all legal regulations, *inter alia*, those concerning crisis management and the protection of classified information.

The risk-assessment approach is an integral element of risk management which, according to the generally acceptable standards, includes risk assessment which covers risk identification; risk analysis and evaluation; decision-making; risk handling; and monitoring and reviewing, whereas

This process concerns any risk and must form an integral part of an organisation's practical activities, and must have an executor capable of providing the appropriate methods and tools for its implementation.²²

Risk assessment (or risk estimation, as in Article 2(13) of the NCSA), according to the generally applicable rules, should thus cover selecting risk sources (incidents) or threats which have or could have an adverse impact on cybersecurity; identifying and creating a list of risks influencing cybersecurity objectives; determining the consequences for information systems of any actions which violate confidentiality, integrity, availability, and authenticity of processed data or the related services provided through such systems; defining the causes of the sources of risks and threats; assessing the efficiency of existing security systems; determining the location, time, and circumstances of risk occurrence; and risk classification in comparison with acceptable values.²³

The development and implementation of a risk-assessment methodology at the national level is considered a priority in the specific objective of the Strategy regarding the establishing of a National Cybersecurity System. Accordingly, "A joint static and dynamic risk-assessment methodology which takes into account the specificity of individual sectors, critical-infrastructure operators, operators of essential services, and digital service providers, shall be introduced for the purpose of cybersecurity management at the national level. This shall ensure the comparability of estimates, also regarding risk levels, in particular for the purpose of national--security-risk reports, developed in accordance with the crisis-management regulations. Risk assessment shall become a continuous process which will enable the identifying of the risk level in near real time.

²²See D. Wróblewski (2015), p. 37.

²³More on the issue, *ibid.*, pp. 44–48.

The methodology and tools facilitating static and dynamic risk assessment in communication and information systems are being developed as part of the National Cybersecurity Platform, a project funded by the National Centre for Research and Development; the completion of this work has been scheduled for the end of 2020.²⁴

7 Educational, Informational and Training Programmes in the Field of Cybersecurity

Activities related to educational, informational, and training programmes in the field of cybersecurity constitute an integral part of the Strategy. This wording has been slightly altered, and seems less precise, compared to the provisions of the NIS Directive, as the latter stipulates that it concerns guidelines referring to programmes developed in this field. In fact, this definition is *more* specific, as these are executive bodies which conduct specific educational, informational, and training activities consistent with their range of competence. The Council of Ministers should provide indications, within the Strategy, regarding the general principles of implementing various undertakings in this area.

The legislators have entrusted duties in the reference scope to numerous entities in the national cybersecurity system, in accordance with their expertise. The major players include the Minister competent for computerisation (see the commentary to Article 45(1)); the Single Point of Contact (Article 49(1)); CSIRT MON, CSIRT NASK and CSIRT GOV (Article 26(3)); and the Minister of National Defence (Article 51).

Cybersecurity tests and audits will be a no-less-important undertaking, and a vehicle for implementing the Strategy. Periodic audits are among measures which allow the assessment of the effectiveness of the currently implemented information security management systems, and the adequacy of the safeguards introduced. Audit methodologies should take into account the applicable standards, good practices, and specificity of the respective sectors. The aim of such an approach is to achieve comparability in audit outcomes. Periodic tests (including penetration testing), which provide for a real assessment of the system's resilience to threats, are another security assessment measure. The outcomes of these tests are the basis for the verification of the safeguards deployed. In order to utilise the public capacity in the sphere of cybersecurity, so-called bug bounty testing will be disseminated, which is a search for software vulnerabilities conducted by people not associated with the software developer, usually with the general consent of the developer.

²⁴See the Cybersecurity Strategy of the Republic of Poland for 2019-2024...op. cit., p. 13.

8 Developing, Reviewing and Updating the Strategy

Article 69 indicates that the Strategy was to be developed for a five-year period with possible amendments throughout its duration. While the document will remain in force for 5 years, it is to be reviewed (in terms of up-to-dateness) every 2 years. At the strategic level, the process of developing long-term tactics oriented towards identifying and implementing organisations' objectives usually takes no less than 5 years, at the tactical level 2–5 years, and at the operational level up to 2 years. The Strategy, reflecting the arrangements made by leading entities in the field of cybersecurity, including the Council of Ministers, which has adopted it by way of a Resolution, is a document of strategic significance. Hence, its duration is 5 years. The legislator, however, has envisaged amendments to be made within its content, on an as-needed basis, and at any time, and its review at an arbitrarily set time, i.e. every 2 years (Article 71 of the NCSA).

It should be stressed once more that, in the case of this Strategy, we are dealing with quite an innovative approach by the legislator in assigning a status to a document which had not previously occurred in the processes of developing and announcing cybersecurity strategies. To date, a similar requirement to determine strategic objectives, and the appropriate political and regulatory measures, to indicate the sectors referred to in Annex 1 to the Act, as well as digital services and public entities, and to specify the leading specific content of the Strategy, its duration and reviews, has not been included in any other strategies regarding national security, national defence, or military strategies.

In 2015, following amendments to the Act of 4 September 1997 on Government Administration Departments,²⁵ the scope of this department was made to include cybersecurity issues. Following the adoption of the NCSA, another amendment was made to the Act on Government Administration Departments, which involved new wording for Article 12a(1)(10). In consequence, the scope of the computerisation department was limited to civil matters related to cybersecurity,²⁶ while its military aspects became the domain of the defence department.

This way, the Minister's leading role in Strategy development arises from the duties assigned to the Ministers chairing specific government administration departments, which involve initiating and developing the Council of Ministers' policies for given departments, and submitting initiatives, draft assumptions, draft Acts, and draft versions of normative Acts, at Council of Ministers meetings, on the principles and according to the procedure defined in the Internal Work Regulations of the Council of Ministers (Article 34(1) of the GAD Act). We are, therefore, dealing with the principle of competency, according to which each body has a set of rights and obligations determined in systemic regulations.

²⁵ Act of 4 September 1997 on Government Administration Departments, Consolidated text Polish Journal of Laws of 2020, item 1220, as amended.

²⁶ See Article 12a (1) and Article 19(1)(1a) of the Act on Government Administration Departments.

The Act indicates the Minister competent for computerisation as the leading body entrusted with developing draft versions of the Strategy. However, given the systemic expertise of the Government Plenipotentiary, other Ministers, and the authorised managers of central offices, and in particular their responsibilities within the national cybersecurity system, cooperation with them is justified for substantive reasons, and in view of the related scope of responsibilities of administration bodies in this field. The Minister can also collaborate with members of the Council of Ministers and government administration authorities to act for the common good and in the public interest, on the principles and according to the procedure defined in the NCSA.

It is also worth stressing that, although the legislators have not specified this issue in the Act, the NIS Directive, and more specifically Article 7(2) thereof, stipulates that Member States may request the assistance of ENISA (the European Union Agency for Cybersecurity) in developing national strategies on the security of network and information systems.

While the work on the draft version of the Strategy can also be attended by a representative of the President of the Republic of Poland, the legislators have not determined who, and under which procedure, decides on the need for the President's representative to be involved. Nor has it been expressly stated that the role of that representative should be fulfilled by the Head of the National Security Bureau.

Under Article 126 of the Constitution of the Republic of Poland, the President is the supreme representative of the Republic of Poland, and the guarantor of the continuity of state authority, who ensures the observance of the Constitution, and safeguards the sovereignty and security of the state, as well as the inviolability and integrity of its territory. Our interest, however, focuses especially on the President's role in the international affairs of the Republic of Poland, as an authority safeguarding national security. Also in this field, the President collaborates with the Council of Ministers as a whole, and with individual Ministers as Council members. Due to the convergence of capabilities, and at the same time their separation, the Minister competent for computerisation, by inviting a representative of the President of the Republic of Poland to attend work on the draft version of the Strategy, contributes to a reliable and efficient operation of public institutions.

The Strategy is of key significance for national security, and for compliance with international obligations. As a result, given the stature of the body which adopts it (the Council of Ministers) and the competences of the President of the Republic of Poland regarding national security, and the cooperation obligation of executive bodies, including when they act through their representatives, in the field of national and EU cybersecurity policies, reflects the implementation of the constitutional principle of collaboration, and avoidance of competition between, public authorities.

Article 71 of the NCSA stipulates that the Minister competent for computerisation, in cooperation with the Plenipotentiary, other Ministers, and the appropriate managers of central offices, shall review the Strategy every 2 years. The authority of this body arises from its being entrusted by the legislator with a mission to develop the draft version of the Strategy in cooperation with the entities indicated in Article 70 of the said Act.

In addition, the periodic character of the Strategy reviews arises from the provisions of the NIS Directive, *inter alia*, on updating the list of identified digital service providers (at least every 2 years), and on the reviewing of the Directive by the European Commission, and reporting to the European Parliament and the Council.

Article 7(3) of the NIS Directive stipulates “Member States shall communicate their national strategies on the security of network and information systems to the Commission within three months from their adoption.” As a result, the Polish legislator has obligated, under Article 72 of the NCSA, the Minister competent for computerisation to submit the Strategy to the European Commission within 3 months of its being adopted by the Council of Ministers.

References

- Ganczar M (2017) Umowne partnerstwo publiczno-prywatne w kontekście bezpieczeństwa sieci i informacji administracji publicznej in: Internet. Strategie bezpieczeństwa, ed. G. Szpor, A. Gryszczyńska, Warsaw
- Wróblewski D (ed) (2015) Zarządzanie ryzykiem - przegląd wybranych metodyk, Józefów

Waldemar Kitler Professor, Eng., full professor at the National Security Faculty of the War Studies University. In scientific activity, he deals with issues of national security, national defense and crisis management as well as selected legal and administrative aspects of security and defense of the Republic of Poland. He has extensive professional experience, including work in universities and central administration. The most important experiences include work at the National Defense University, the Department of Defense System of the Ministry of National Defense, the Office of Crisis Management and Civil Protection and the National Headquarters of the State Fire Service. In the years 2010–2011 he managed the Cathedral of Law and Administration. From 2011, he was the Vice-Dean of the Faculty of National Security for Scientific Affairs. In the years 2015–2016 he was the head of the Cathedral of National Security Law, and in the years 2017–2019 the director of the Institute of Law and Defense Administration. Currently, he is the director of the Institute of State Security. The professor promoted 16 doctors and his scientific achievements include over 260 publications, including over 80 articles and scientific papers, 25 original creative works (including 10 monographs), about 60 scientific and research papers, 8 textbooks and academic scripts, 90 reviews and scientific opinions.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.