*Polish Political Science Yearbook*, **vol. 52(3) (2023), pp. 155–163**
DOI: https://doi.org/10.15804/ppsy202383 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

**Mirosław Karpiuk**
University of Warmia and Mazury in Olsztyn (Poland)
ORCID: 0000-0001-7012-8999
e-mail: m_karpiuk@wp.pl

**Anna Makuch**
University of Economics and Human Sciences in Warsaw (Poland)
ORCID: 0000-0002-5222-4407
e-mail: a.makuch@vizja.pl

**Urszula Soler**
The John Paul II Catholic University of Lublin (Poland)
ORCID: 0000-0001-7868-8261
e-mail: urszula.soler@kul.pl

# The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity

**Abstract:** Cybersecurity belongs to the area of activity of state and supra-state actors, giving direction to national and international systems of law as components of national and supranational systems of political, economic, military cooperation, etc. Still, the state has a monopoly on the causality of lawmaking, which forms the basis of cyberspace use security activities. The state responds to national security needs by actively participating in the formation of the collective security order of the supranational level. The aim of this paper is to demonstrate the significance of the national Cybersecurity Strategy of the Republic of Poland for ensuring the safe use of cyberspace. The Strategy, while referring to the national order, is at the same time an implementation of supranational arrangements within the scopes adopted by the state authorities, which means that the Strategy is subjected to logical evaluation depending on the impact of cyber conditions or binding arrangements of the international environment. The text is based on two research methods: the doctrinal legal research method to analyse the applicable legal regulations governing the issues related to the strategic aspects of cybersecurity and the law theory method aimed at evaluating the strategic solutions in respect of security in cyberspace.

***Keywords:*** *social security, cyberspace, cybersecurity, public security, cybersecurity strategy*

## Introduction

The protection of security in cyberspace constitutes one of the most important tasks entrusted not only to public sector entities but also to the private sector since not only our public and professional lives but also our private lives very often revolve around online activities. Progressing digitisation has placed the meta-medium of the internet at the centre of operations pursued by individuals as well as state and non-state entities. Cyberspace users use its resources and generate new resources for economic, informational, political and other purposes, contributing directly and indirectly to the evolution of the digital environment with new tools, innovations and solutions that facilitate users' activities. The internet has become a nervous system of sorts, driving revolutionary transformation in every sphere of human activity (Castells, 2013). It has, on the one hand, become a tool facilitating our functioning through time and space, and, on the other, a certain standard operational setting (even for local businesses).

To conduct certain types of activities (including economic or educational ones) in an uninterrupted way, we need to secure our ICT systems. This also applies to situations where a service provider offers entertainment. In the era of digital states and information societies, widely used ICT systems must be appropriately protected. Failure to provide such protection may undermine citizens' trust in public authorities. They must not only take actions to provide cybersecurity but compel private entities to apply appropriate safeguards so that cyber-attacks do not hinder the operations of institutions representing both sectors (public and private).

Under Article 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws of 2022, item 1863, as amended) — further referred to as the NCSA, the Polish legislator defines cybersecurity as "the resilience of information systems (information and communications systems with electronic data stored therein) against actions which compromise the confidentiality, integrity, availability and authenticity of processed data, or the related services provided by those information systems. Because cybersecurity refers to the ability to resist disruptions in ICT systems (Czuryk, 2022b, p. 106), it constitutes a special security system component which covers the protection of those systems against threats (Czuryk, 2019, p. 42).

The state implements a cybersecurity policy by taking strategic and operational measures, including actions responding to specific (individual) incidents, depending on the status of such incidents. Strategic measures are implemented at the level of specific technical actions aimed at securing cyberspace, as well as at the normative and planning levels related to the drafting of specific legal acts and documents across various levels of the legal system. Examples of such documents include the National Security Strategy of the Republic of Poland (Warsaw, 2020), further referred to as the Security Strategy, and the Cybersecurity Strategy of the Republic of Poland for 2019-2024 (Resolution of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019-2024, Official Gazette of the Republic of Poland "Monitor Polski" of 2019, Item 1037) – further referred to as the Cybersecurity Strategy.

The objective of this paper is to demonstrate the significance of the national Cybersecurity Strategy of the Republic of Poland for ensuring the safe use of cyberspace. The doctrinal legal research method was applied in this study. It was used to analyse applicable legal regulations governing the issues related to the strategic aspects of cybersecurity. The law theory method was applied to a narrower extent, mostly with the aim of evaluating strategic solutions in respect of security in cyberspace.

## Security in cyberspace

Cyberspace is understood as a space for the processing and exchange of information created by ICT systems, including the links between them and their relations with users – as per Article 2(1b) of the Act of 29 August 2022 on Martial Law and the Competencies of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws of 2022, item 2091). It is a place where public, private, social and economic activities are conducted. And, since it serves the provision of various types of services and communications, it is significant both to the state and to society. Therefore, cyberspace must be duly protected (Karpiuk & Kelemen, 2022, p. 71). The need for its protection results not only from its essential significance for the functioning of public institutions but also from the development of an information society which widely uses various means of communication relying on ICT systems (Karpiuk, 2021b, p. 241).

The notion of security, in the philosophical sense, means the certainty of survival, the elimination of threats, and development opportunities in line with independently adopted tactics and operational measures. The issues of the security of humans and their environment have become increasingly complex since the early 19th century. This development has been correlated with a notable increase in the significance of international relations at regional and global scales – a process driven by such drivers of change as the industrial revolution, the political uprisings of the late 18th century and early 19th century, and a number of innovations introduced in the 19th and 20th centuries (Skrzypek, 2009). The internal security of state entities was, to a growing extent, dependent on regional security and sound international relations (Dobrzycki, 2004).

In security sectors, the objective catalogue has been greatly extended across the centuries, and it is difficult to consider the list as exhaustive given the dynamics and polyarchy of the contemporary international environment; the tasks which states need to perform include previously unknown or disregarded ecological, sanitary, demographic, and cultural security, making it necessary to extend national security strategies and political programmes by incorporating issues which give rise to reasonable concerns. Legal and political entities included captivating issues in system-related activities in a processual way through national legislation, the structures of relevant central or local level agencies, and the distribution of responsibilities and powers. The improvement of the state system was influenced by ideas and social and political circumstances, including economic and political crises.

Due to the significance of cyberspace, whose impact is described as revolutionary, the security of its use was introduced in the workflows of system-related tasks of state entities due to multiple subjective levels, i.e., individual (personal), group (family), national (state) and international (bilateral, regional and global) levels. The structure of security systems includes the physical, technical, legal and institutional levels, and as regards information security – the cultural and psychological factor; it should be noted, however, that the dimension of international cooperation constitutes an integral part of cyberspace security due to the transnational reach of the internet, and its impact on communication, cooperation and competition processes, deepening globalisation. Cybersecurity systems correspond to the range and scale of cyberspace itself, although in an orderly way in terms of setting standards and developing cooperation rules, for which the formal law system continues to be relevant. The network of cooperation systems related to cyberspace security brings together various entities at horizontal and vertical levels, state systems, and private and public users, striving for integration and efficiency of operations for a collective cybersecurity system.

## The strategic context of cybersecurity

As a result of transformations of the security environment throughout the ages, the main global trends have been towards the extension of security catalogues of individuals and the state, the mitigation of the military factor and the increase in intangible factors, among which the digital environment has become one of the key spheres of system-related state operations. Due to the cybersecurity of the state, distinct emphasis should be placed on counteracting incidents which have or might have a negative effect on the operations of information systems, particularly severe and critical incidents (Karpiuk, 2022b, p. 407). As per Article 2 (6) of the NCSA, a critical incident is an incident which results in significant damage to security or public order, as well as international interests, economic interests, the operations of public institutions, civil rights and liberties, or human lives and health. In turn, under Article 2(7) of the NCSA, a serious incident means an incident which results, or might result, in a severe decrease in the quality of an essential service or disrupt its continuity. The level of preventive and counteractive measures, through appropriate design of ICT networks together with a system of safeguards, remains in a direct relationship to the level of consequences of an incident compromising network security; in such an event, a state institution whose teleological objective is the security of a political community has the right and obligation to use legal or judicial measures to restore the state security and balance (in a purely normative sense) in place before the occurrence of the incident. The anticipation of threats, and the response to existing ones, constitute complementary tactical and operational actions in the domain of cyberspace at institutional and state levels.

State cybersecurity is a strategic objective which must be considered not only across all sectoral fields of state activity and public policy but also in the sphere of independent business activities or the social sphere. Cyberthreats are multidimensional, hence the activities aimed at combating them must be well-coordinated, as well as deployed at all levels of the state's administrative division, in the economic sphere (in particular when operators of essential services and digital service providers are concerned), and in the social sphere (with various degrees of intensity, of course). It is vital to keep such activities commensurate with the degree of a given threat.

Cyber-attacks might give rise to various types of negative phenomena resulting in crises, in particular, if they are targeted against ICT systems through which the state is fulfilling its strategic objectives, including the ones related to ensuring the continuity of operation of critical infrastructure (having fundamental importance for the continuity of supplies and services). Threats in cyberspace might lead to crises, as the activities of both public and private institutions are also, to a great extent, performed in cyberspace, and the ICT systems that they use are not always duly secured (Karpiuk, 2022a, p. 114).

The Cybersecurity Strategy points to the need to improve the level of resilience against cyber threats, increase the level of information protection in the public, military and private sectors, and promote knowledge and good practices to help citizens better protect their information.

The Cybersecurity Strategy of the Republic of Poland is adopted by the Council of Ministers, as stipulated in Article 68 of the NCSA. Article 69 of the NCSA defines strategic objectives and relevant political and regulatory measures designed to reach and maintain a high level of cybersecurity. It takes into account, in particular: 1) the objectives and priorities in the sphere of cybersecurity; 2) entities engaged in strategy implementation and execution; 3) measures aimed at the fulfilment of its objectives; 4) the definition of actions in respect of preparedness, response and restoration of the normal status, including rules of cooperation between the public and the private sectors; 5) the approach to risk assessment; 6) activities related to educational, informational and training programmes concerning cybersecurity; 7) activities involving research & development plans in the area of cybersecurity. The strategy is adopted for a five-year period, during which it may be revised.

The strategies constitute critical, binding and recommended security agendas and national law documents prepared as a result of the response to challenges arising from the use of cyberspace. The impulse to introduce a given format of cybersecurity strategy comes from observations and conclusions derived from the way cyberspace is used, pointing to threats and risk factors related to such use. The conclusions formulated based on the collected materials at national and international levels serve the preparation of legitimate generalisations and recommendations to provide efficient preventive measures and responses to ensure cyberspace security. The strategies reflect the trends in cyberspace evolution and the ways it is used. Presently, they belong to standard national law tools guiding action in this field.

Domestic security levels continue to be closely related to the level of international cooperation and the nature of existing alliances. It is currently assumed that the international environment constitutes one of the strongest impulses to state systems due to, among others, the transnational dimension of problems, such as cyberspace security, terrorism, global-scale speculative operations, and consequently coordinated activities of state and non-state entities (which were playing an increasingly important role in international relations throughout the 20th century). The significance and influence of alliances on the policies of their member states are a consequence of the weight and power of state signatories, which is possible to estimate based on their effect on the social and political reality and their ability to effectively assert their interests and needs. In the European region, the integrative and political alliance of the European Union is critical to the formulation of state policies under primary and secondary EU law. The North Atlantic Treaty Organisation, belonging to a group of defence alliances and constituting one of the main pillars of the security of the Republic of Poland, is also a vital alliance. Poland actively supports, and participates in, several more or less formal international cooperation networks (e.g. the Council of the Baltic Sea States, the Visegrad Group) dedicated to sectoral or collective security. Cooperation at the transnational level is a dominant trend in the activities of state entities aimed at promoting their values and interests.

Taking into account the problems and challenges of the EU, the NIS Directive was prepared and adopted (Wrzostek, 2016), to be further extended and updated by the NIS2 Directive (Szczęsna, 2022). It should be stressed that the international nature of security, including cybersecurity, is expressed in the transnational nature of legislative initiatives that are less formalised and embedded in the international environment than at the national level. The guidelines and recommendations laid down in the NIS Directive were incorporated in Poland in the National Cybersecurity System Act (2018). This way, the provisions of national law, taking into account the geopolitical specificity of Poland, at the same time provide the basis for the development of the EU's legal system, aimed at integrating preventive and response measures.

The primary objective of the Cybersecurity Strategy is to improve the level of resilience to cyber threats, increase the level of information protection in the public, military and private sectors, and promote knowledge and good practices to help citizens better protect their information. Specific objectives include: 1) developing the national cybersecurity system, 2) increasing the level of resilience of information systems operated by public administration and the private sector, and providing the capability to effectively prevent and respond to incidents; 3) boosting the national potential in cybersecurity; 4) raising awareness and social competencies in the sphere of cybersecurity; 5) building a solid international position of the Republic of Poland in the sphere of cybersecurity. The priority, therefore, is to secure the public (including the military) as well as the private – since private entities have a significant impact on the functioning of the state – sectors against threats.

On the first point, it is worth stressing that the national cybersecurity system is integrated with external partners and yet, at the same time, separated. It constitutes a digital matrix of the government and local government administration system, whose tightness and impenetrability by unauthorised parties constitutes an object of special attention on the part of state security services. On the second point, the legislator indicated the need to improve the efficiency of adjusting security systems to align it with the degree of creativity and advanced knowledge of cybercrime perpetrators. It is worth noting that emphasis has been placed on the competencies related to the logic and critical analysis of the contents provided by, for instance, electronic mail systems to private users. In this case, the selection and classification of threats are made by a cautious recipient, not firewalls. The assumptions of the third point direct our attention to the processual nature of using network tools which are constantly evolving and require the proportional engagement of competent civil and uniformed services and, as indicated in Point 4, the call for taking responsibility for cyberspace security addressed to both state institutions and private entities. Cyberspace is an egalitarian domain of activity. It is a forum for the exchange, production and export of data across all subject areas. Hence the republican component of the engagement and development of not only technical navigation skills but also the ability to critically analyse data and content is warranted.

The national potential in cybersecurity has been considered to be a promising factor for reinforcing the position of Poland on the international stage. As a result of the industrial and digital revolution, the centre-periphery model has undergone significant changes, as colonial, cultural or industrial factors are no longer prevailing in the hierarchies within the international environment. Nowadays, digitally excluded entities are considered peripheries, while the centre is occupied by states that are leaders in technological development, digital solutions and innovation.

As the title suggests, the Cybersecurity Strategy directly influences public administration entities and – upon the adoption of generally applicable legal regulations of the Council of Ministers – other public authorities, enterprises and citizens. However, for the Strategy to have an indirect external effect, the adopted solutions must also be incorporated into acts of generally applicable law because strategic documents are internally binding regulations.

## Conclusions

The cybersecurity challenge creates the need to take into account situations which are not necessarily reflected in the real world. The notion of cybersecurity may refer to the spheres related to information security, communication security or the security of a given ICT system itself (K. Chałubińska-Jentkiewicz, 2019, p. 13). ICT systems are not only useful for searching for information but also for communications, conducting business activities, providing various types of services, and performing public tasks. Their importance for the public and business sectors means the highest priority in certain circumstances. This leads to the implementation of appropriate measures ensuring due protection. In some situations, this might also result in the restriction of human liberties and rights (Czuryk, 2022a, p. 40).

It should be stressed that the possibilities offered by digital technologies are also used for adverse activities, including unfair competition practices, disrupted provision of digital services, offences committed with the use of the internet, or terrorist operations (Kostrubiec, 2022, p. 8). Cyberspace also constitutes a domain of active operations of international actors (Makuch, 2020) for which it is a place where data is acquired and exported, a channel of multi-layered disinformation operations and an effective form of influence on the public opinion, which might consequently give rise to protests or even social unrest (as in the case of protests against the deployment of 5G technology in Europe) (Soler, 2022).

When drafting some of the planning documents, public administration authorities need to account for cybersecurity as one of the elements which ensures the efficient performance of public tasks requiring protection against cyberthreats. Planning, which also takes cyberspace into consideration, allows coordinated actions aimed at the effective and timely accomplishment of public objectives set by administration authorities in a well-organised and continuous way. At times, this requires the engagement of multiple entities (Karpiuk, 2021a, p. 46). It is necessary to allow the state to function safely, also in cyberspace, and to be able to provide security to its citizens.

**References:**

Castells, M. (2013). *Władza informacji*, transl. W. Jedliński, P. Tomanek, PWN.

Chałubińska-Jentkiewicz, K. (2019). Cyberbezpieczeństwo – zagadnienia definicyjne. *Cybersecurity and Law*, *2*(2), 7–23. DOI: 10.35467/cal/133828

Czuryk, M. (2019). Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity. *Cybersecurity and Law*, *2*(2), 39–50. DOI: 10.35467/cal/133839

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

Czuryk, M. (2022b). Special rules of remuneration for individuals performing cybersecurity tasks. *Cybersecurity and Law*, *8*(2), 105–112. DOI: 10.35467/cal/157128

Dobrzycki W (2004)., *Historia stosunków międzynarodowych w czasach nowożytnych*, Scholar.

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

Karpiuk, M. (2021b). The Organisation of the National System of Cybersecurity: Selected Issues. *Studia Iuridica Lublinensia*, *30*(2), 233–244. DOI: 10.17951/sil.2021.30.2.233-244

Karpiuk, M. (2022a). Crisis management vs. cyber threats. *Sicurezza, Terrorismo e Societa*, *16*(2), 113–123.

Karpiuk, M. (2022b). The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights. *Przegląd Prawa Konstytucyjnego*, *67*(3), 401–412. DOI: 0.15804/ppk.2022.03.30

Karpiuk, M., Kelemen, M. (2022). Cybersecurity in civil aviation in Poland and Slovakia. *Cybersecurity and Law*, *8*(2), 70–83. DOI: 10.35467/cal/157125

Kostrubiec, J. (2022). Cybersecurity System in Poland. Selected Issues. In: M. Karpiuk, J. Kostrubiec (Eds.), *The Public Dimension of Cybersecurity* (pp. 7–17). Maribor: LEX Localis Press. DOI: 10.4335/2022.1.

Makuch A. (2020). Twitter jako narzędzie współczesnej dyplomacji – miejsce nowych mediów w procesie kształtowania ładu międzynarodowego, *Karpacki Przegląd Naukowy*, *3-4*(34), 13–27.

Skrzypek A. (2009). *Historia społeczna Europy XIX i XX wieku*, Wydawnictwo Poznańskie.

Soler, U. (2022). Social perception of 5G technology. *Rocznik Instytutu Europy Środkowej i Wschodniej*, *20*(2022), 103–120.

Szczęsna A. *Nadzór nad podmiotami kluczowymi i ważnymi w dyrektywie NIS 2.* https://cyberpolicy.nask.pl/nadzor-nad-podmiotami-kluczowymi-i-waznymi-w-dyrektywie-nis2/

Wrzosek M. *Dyrektywa NIS, czyli pierwsze europejskie prawo w zakresie cyberbezpieczeństwa.* https://cyberpolicy.nask.pl/dyrektywa-nis-czyli-pierwsze-europejskie-prawo-w-zakresie-cyberbezpieczenstwa/