Mirosław Karpiuk*

The Cybersecurity Strategy of the Republic of Poland as a Source of Internal Law

Abstract

Cybersecurity as a subject of regulation can be found in a number of legal acts, both generally applicable and internal. This type of regulation is also found in the Cybersecurity Strategy of the Republic of Poland. The Strategy, however, as an act of internal law, has limited power. It does not influence external entities and, therefore, cannot form grounds for individual decisions relating to citizens, entrepreneurs, and other entities. Its primary objective of increasing the level of resilience to cyberthreats should be a priority for the state policy.

Key words: cybersecurity, cyberspace, internal law

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

Cyberspace has become the most rapidly developing area of the infosphere, an area that is not territorially defined. It is dispersed among ICT systems and data collection infrastructure. Thus, physically, we can speak of IT devices and software enabling the processing and storage, as well as the sending and receiving of data. These, in turn, are dispersed not only within a single country, but also across the world. The data processed by ICT systems represent information that creates, sustains and modifies social relations. Cyberspace is vulnerable to unauthorised modifications of data and the messages they create. This leads to the dangers posed by possible interference with the form and content of the messages sent by the sender to the addressee at the stage of processing and circulation of data in cyberspace. Another type of danger resulting from the use of cyberspace to transmit information is the speed and ease with which unauthorised messages can be routed to addressees. These can be forged even before the stage of entering cyberspace. The speed, accessibility and limited accountability associated with the circulation of information in cyberspace make it the area of the infosphere that is ideally suited for the transmission of false content[1]. Given the importance of cyberspace, its protection is the subject of many acts, including strategies. They indicate, *inter alia*, the need to increase resilience to cyberthreats and to boost information protection in the public, military and private sectors, as well as fostering knowledge and good practices enabling citizens to better protect their information[2]. Cyberspace is generating new threats and confronting people with different, previously unknown challenges. It also redefines the security environment and sets new risk parameters. These new threats and their associated risks make it necessary to adequately design countermeasures, taking into account the specificity of the changes taking place[3].

The Cybersecurity Strategy of the Republic of Poland („the Strategy") indicates the priorities for ensuring the security of cyberspace. These priorities should also be part of the state's policy which, in the age of computerisation, must take cybersecurity into consideration.

1 M. Ciesielski, *Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities*, „Cybersecurity and Law" 2024, no. 1, p. 189–190.

2 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, p. 20. See also J. Kostrubiec, *Authorities Competent for Cybersecurity and Their Operational Strategies* [in:] *Information, Disinformation, Cybersecurity*, eds. K. Chałubińska-Jentkiewicz, O. Evsyukova, Toruń 2023, p. 154.

3 K. Drabik, *Cyberprzestrzeń – zagrożenia i wyzwania* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024, p. 9.

The Polish legislator defines cybersecurity as the resilience of information systems to any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[4]. As stated by the EU legislator, the security of network and information systems means the ability of these network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems[5]. Cybersecurity means the actions necessary to protect network and information systems, users of such systems and others from cyberthreats[6].

4 Art. 2(4) of the Act of 5 July 2018 on the National cybersecurity system (consolidated text, Journal of Laws 2023, item 913 as amended.), hereinafter: the ANCS.

5 Art. 4(2) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (Official Journal of the European Union 2016, L 194, p. 1).

6 Art. 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (the Cybersecurity Act) (ibidem 2019, L 151, p. 15). For more information about cybersecurity, refer to: M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; A. Żebrowski, *Cyberprzestrzeń miejscem walki (wojny) informacyjnej (wybrane aspekty)* [in:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, eds. J. Grubicka, A. Kamińska-Nawrot, Słupsk 2020; A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2; I. Hoffmam, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1; M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5; K. Kaczmarek, *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1; J. Kulesza, *Należyta staranność a cyberbezpieczeństwo wewnętrzne organizacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. P. Dziuba, Warszawa 2023; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2; A.E. Patkowski, *Walka w cyberprzestrzeni. Refleksje po przeglądzie incydentów* [in:] *Metody i narzędzia w procesie tworzenia cyberzdolności – wyzwania i perspektywy*, Warszawa 2022; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

The Strategy is a document where specific objectives related to cybersecurity are planned to be implemented. It is these objectives that public administration, including in particular government administration, should pursue.

One of the key roles played by public administration is that connected with planning. This is why its various bodies, regardless of whether they operate in a particular area or in the entire national territory, are obliged to draw up various types of plans, strategies or programmes. Sometimes they have to take into account cybersecurity as an important element in their planning documents to ensure efficient performance of the public tasks that need to be protected against cyberthreats. Planning, including that related to cyberspace, makes it possible to take coordinated action allowing for the proper, timely and harmonious implementation of the objectives set for public administration in an organised and continuous manner, especially with the involvement of many entities of different nature[7].

The Cybersecurity Strategy of the Republic of Poland is a development strategy based on which development policy is pursued. The legislator understands development policy as a set of interrelated activities undertaken and implemented to ensure sustainable and balanced development of the country, to foster socio-economic, regional and spatial cohesion, to increase economic competitiveness, and to create new jobs on the national, regional or local scale[8]. It belongs to the category of „other development strategies" which are defined, under Art. 9(3) of the APDP, as documents determining the basic conditions, objectives and directions of development, relating to sectors, disciplines, regions or spatial development. One of the authorities that pursue the development policy is the Council of Ministers.

As stipulated in Art. 68 of the ANCS, the Council of Ministers adopts the Strategy by way of a resolution. Resolutions of the Council of Ministers are applicable internally, i.e., they are binding only on the organisational units subordinate to the issuing body[9]. Acts of internal law cannot contain

7 M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, p. 46.

8 Art. 2 of the Act of 6 December 2006 on the Principles of Development Policy (consolidated text, Journal of Laws 2024, item 324, as amended), hereinafter: the APDP

9 Art. 93 of the Constitution of the Republic of Poland of 2 April 1997 (ibidem 1997, no. 78, item 483, as amended). Ensuring digital security is one of the basic tasks of public authorities. See K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 145.

universally binding norms, as they are only addressed to the organisational units subordinate to the issuing body, which significantly narrows their subjective scope of application. Consequently, acts of internal law cannot regulate issues which are reserved for the matters covered by universal acts of law, regulations or local laws, and thus they cannot interfere with individual rights and freedoms. Acts of internal law do not constitute the basis for decisions and similar rulings with respect to citizens, legal persons and other entities[10].

The constitutional regulation of the place of internal acts in the legal system has been limited through adopting the principle that they are to comply with universally applicable law, without determining their hierarchy. Decisive in this respect will be the legally defined relations of supremacy and subordination of the bodies issuing such acts[11].

Under Art. 69 of the ANCS, the Strategy sets out strategic objectives, and relevant political and regulatory measures, to achieve a high level of cybersecurity. It takes into account, in particular: 1) cybersecurity objectives and priorities; 2) entities involved in its implementation and deployment; 3) measures used to achieve the set objectives; 4) specification of means for readiness, response and restoration, including the principles of public-private cooperation; 5) a risk assessment approach; 6) activities related to educational, information and training programmes regarding cybersecurity; and 7) activities related to research and development plans regarding cybersecurity. The Strategy is adopted for a five-year period with the possibility of amendments during the period of validity. As recognised by the legislator, given the dynamics of the changes taking place in cyberspace, the five-year period of validity of the Strategy is long enough for the document to require an update.

The underlying objective of the Strategy is to increase resilience to cyberthreats, to boost information protection in the public, military and private sectors, as well as to foster knowledge and good practices enabling citizens to better protect their information. Its specific goals include: 1) developing the national cybersecurity system; 2) increasing the level of resilience of information systems of the public administration and private sector, as well as achieving the capacity to effectively prevent and respond to incidents; 3) increasing the national capacity in the area of cybersecurity

10 P. Radziewicz [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. P. Tuleja, Warszawa 2023, Art. 93.

11 B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, p. 469.

technology; 4) building public awareness and competences in the area of cybersecurity; and 5) building a strong international position of the Republic of Poland in the area of cybersecurity. The Strategy clearly indicates that it is essential to improve the efficiency of the national cybersecurity system, and thus it is important to use an ICT system supporting: 1) cooperation of entities involved in the national cybersecurity system; 2) generation and transfer of recommendations of activities increasing the level of cybersecurity; 3) incident reporting and handling; 4) risk assessment at the national level; and 5) cyberthreat warnings. It is noted that, in order to increase the resilience of the information systems used by the public administration to cyberthreats, it is necessary to develop cybersecurity standards as a set of organisational and technical requirements regarding, in particular, the security of: 1) applications; 2) mobile devices; 3) workstations; 4) servers and networks; and 5) cloud computing models. It is emphasised that ensuring security in cyberspace requires joint efforts of the private sector, the public sector and citizens. In this regard, it is necessary to continue building an effective public-private partnership system based on trust and shared responsibility for cybersecurity. The Strategy also draws attention to raising the competences of the staff in charge of ensuring cybersecurity in Poland, assuming that this should be done through establishing and introducing a model of academic education and professional development that will ensure the appropriate qualifications of specialists in this area of practice. To this end, model academic programmes are to be developed for a dedicated field of cybersecurity. The current version of the Strategy focuses on active international cooperation at the strategic and political levels. Given the widespread globalisation processes and related interdependence of states, international cooperation is essential for achieving security in global cyberspace. In carrying out tasks at the European level, Poland should intensify its efforts to ensure the security of the European Union's single digital market, as a factor allowing economic growth and innovation. It is also important to strive for a broader inclusion of cybersecurity aspects in attempts at deepening the European Union's Common Foreign and Security Policy[12].

12 Cybersecurity Strategy of the Republic of Poland for 2019–2024, constituting an annex to Resolution no. 125 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 Government of the Republic of Poland 2019, item 1037). See also: M. Czuryk, *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law"

Improving digital competences, as highlighted by the National Cybersecurity Strategy, is very important for ensuring security in cyberspace. In addition to the appropriate ICT equipment or security software, people have an important role to play in cybersecurity protection, so they must have the appropriate knowledge and skills.

In a state whose operations are based on ICT systems, digital competences are particularly important, both for employees of the administrative apparatus and for the public. These competences allow faster circulation of information, better contact between citizens and the office, and cheaper implementation of public tasks. Relations with the administration, involving the use of digital tools, are much more convenient than those which require face-to-face interactions between the parties. In a changing reality, the computerisation of public activities is becoming inevitable; they must adapt to the new digital circumstances. The information society is not only a society that uses digital tools to interact with public administration, but also one that uses new technologies in everyday life[13]. The level of digital competence has now become one of the most important elements that affect quality of life[14].

The draft Strategy is developed by the minister competent for computerisation, in cooperation with the Government Plenipotentiary, other ministers and heads of the relevant central offices. A representative of the President of the Republic of Poland may also participate in the work on the draft Strategy. These bodies are referred to in Art. 70 of the ANCS.

The draft Strategy is developed by the minister competent for computerisation, hence the minister whose competence includes matters of: 1) computerisation of the public administration and entities performing public tasks; 2) ICT systems and networks of the public administration; 3) support of investments in the field of computerisation; 4) implementation of the international commitments of the Republic of Poland in the field of computerisation and telecommunications; 5) participation in shaping the European Union policy in the field of computerisation; 6) development of the

2024, no. 1, p. 40–41; J. Kostrubiec, op. cit., p. 153; A. Pieczywok, *Kształtowanie świadomości i kompetencji cyfrowych obywateli na przykładzie „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" oraz środowiska szkół* [in:] *Cyberbezpieczeństwo. Aspekty krajowe…*, p. 305–206.

13 A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law" 2024, no. 1, p. 259.

14 K. Kaczmarek, *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats*, [in:] *The Public Dimension…*, p. 30.

information society and counteracting digital exclusion; 7) development of services provided by electronic means; 8) shaping the state's policy in the area of personal data protection; 9) telecommunications; 10) cybersecurity in the civil dimension; 11) the register of Personal Identification Numbers (PESEL), the Register of Personal Identity Cards, the Civil Status Register and the Register of Passport Documents; 12) the register of vehicles, the register of drivers and the register of parking card holders; 13) oversight of the provision of trust services within the meaning of the provisions on trust services; and 14) electronic identification[15]. The minister competent for computerisation is the leading authority in the case of strategy development, but given the competences of the Government Plenipotentiary for Cybersecurity, other ministers and heads of central offices, cooperation with them is justified for substantive reasons[16].

The draft Strategy is prepared in cooperation with the Government Plenipotentiary for Cybersecurity, who reports to the Council of Ministers. The Government Plenipotentiary's tasks, as stipulated in Art. 60 of the ANCS, include coordinating activities and implementing the government's policy on ensuring cybersecurity in the Republic of Poland. Coordinating should be understood as determining interests higher than those of the coordinated entities, which ensures the coherent implementation of the government's policy. The divergence of interests of the various bodies comprising the national cybersecurity system may hinder the achievement of specific goals. Therefore, the coordination instruments assigned to the Government Plenipotentiary for Cybersecurity should be adequate to the needs[17].

The Minister competent for computerisation, in cooperation with the Government Plenipotentiary, other ministers and heads of the relevant central offices, reviews the Strategy every two years. An obligation to do so is stipulated in Art. 71 of the ANCS. The review of the Strategy is carried out within the framework of cooperation by the same bodies that are responsible for its preparation. In both cases, the legislator does not specify how this cooperation should work.

15 Art. 12a the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2022, item 2512, as amended).

16 W. Kitler [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. idem, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 338.

17 G. Szpor [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. eadem, A. Gryszczyńska, K. Czaplicki, Warszawa 2019, Art. 60.

ICT systems are widely used by both private and public entities. They are employed not only for faster communication but also for carrying out tasks, including those of great importance for the proper functioning of the state. Due to their very nature, they must be adequately protected so that any cyberattacks that disrupt their functioning could be headed off or eliminated[18]. These systems contribute to the stability of the state and its economy[19]. As the security of ICT systems, which use cyberspace for their operation, is strategic, the Council of Ministers standardises these issues in the Strategy.

Each Member State adopts a national cybersecurity strategy that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The EU legislator stipulates that the national cybersecurity strategy should include: 1) objectives and priorities of the Member State's cybersecurity strategy; 2) a governance framework to achieve the objectives of the Member State, including the cybersecurity policy; 3) a governance framework clarifying the roles and responsibilities of relevant stakeholders at national level, underpinning the cooperation and coordination at the national level between the competent authorities, the single points of contact, and the CSIRTs, as well as coordination and cooperation between those bodies and competent authorities under sector-specific Union legal acts; 4) a mechanism to identify relevant assets and an assessment of the risks in that Member State; 5) an identification of the measures ensuring preparedness for, responsiveness to and recovery from incidents, including cooperation between the public and private sectors; 6) a list of various authorities and stakeholders involved in the implementation of the national cybersecurity strategy; 7) a policy framework for enhanced coordination between the competent authorities for the purpose of information sharing on risks, cyber threats, and incidents, as well as on non-cyber risks, threats and incidents and the exercise of supervisory tasks, as appropriate; and 8) a plan, including necessary measures, to enhance the general level of cybersecurity awareness among citizens[20].

18 M. Karpiuk, *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2, p. 121.

19 A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 89–90.

20 Art. 7(1) of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972

Solving cybersecurity problems requires not only close but also multifaceted cooperation between individuals, institutions and states, as no single actor can counter threats alone. Such cooperation is most often realised on the basis of common interests between different actors[21]. This cooperation is also prescribed by the European Union legislator and must also find its place in the Strategy.

On the one hand, technological development allows for more efficient and faster performance of tasks, as well as for better communication; on the other hand, it entails risks. Cyberattacks can even disrupt the normal operation of a state, which may suffer significant losses due to their occurrence, which makes ensuring cybersecurity a necessity[22]. This necessity also stems from the Strategy.

Bibliography

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009.

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Bencsik A., Karpiuk M., Strizzolo N., *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law" 2024, no. 1.

Ciesielski M., *Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities*, „Cybersecurity and Law" 2024, no. 1.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Czuryk M., *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Czuryk M., *The Legal Status of Digital Service Providers in the National Cybersecurity System*, „Cybersecurity and Law" 2024, no. 1.

Drabik K., *Cyberprzestrzeń – zagrożenia i wyzwania* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

and repealing Directive (EU) 2016/1148 0000 333 Directive, 80) (Official Journal of the European Union 2022, L 333/80).

21 K. Kaczmarek, *Nordic Countries in the Face of Digital Threats*, „Cybersecurity and Law" 2024, no. 1, p. 152.

22 O. Evsyukova, M. Karpiuk, M. Kelemen, *Cyberthreats in Ukraine, Poland and Slovakia*, ibidem, p. 60.

Evsyukova O., Karpiuk M., Kelemen M., *Cyberthreats in Ukraine, Poland and Slovakia*, „Cybersecurity and Law" 2024, no. 1.

Hoffmam I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2.

Kaczmarek K., *Digital Competencies of the General Public and the State's Vulnerability to Cyberspace Threats*, [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Kaczmarek K., *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1.

Kaczmarek K., *Nordic Countries in the Face of Digital Threats*, „Cybersecurity and Law" 2024, no. 1.

Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., Kelemen M., *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2.

Kitler W. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Kostrubiec J., *Authorities Competent for Cybersecurity and Their Operational Strategies* [in:] *Information, Disinformation, Cybersecurity*, eds. K. Chałubińska-Jentkiewicz, O. Evsyukova, Toruń 2023.

Kulesza J., *Należyta staranność a cyberbezpieczeństwo wewnętrzne organizacji* [in:] *Zagrożenia wewnętrzne bezpieczeństwa zasobów informacyjnych w organizacji*, ed. P. Dziuba, Warszawa 2023.

Patkowski A.E., *Walka w cyberprzestrzeni. Refleksje po przeglądzie incydentów* [in:] *Metody i narzędzia w procesie tworzenia cyberzdolności – wyzwania i perspektywy*, Warszawa 2022.

Pieczywok A., *Kształtowanie świadomości i kompetencji cyfrowych obywateli na przykładzie „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" oraz środowiska szkół* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, ed. M. Karpiuk, Warszawa 2024.

Radziewicz P. [in:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, ed. P. Tuleja, Warszawa 2023, Art. 93.

Szpor G. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019, Art. 60.

Żebrowski A., *Cyberprzestrzeń miejscem walki (wojny) informacyjnej (wybrane aspekty)* [in:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, eds. J. Grubicka, A. Kamińska-Nawrot, Słupsk 2020.

Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej jako źródło prawa wewnętrznie obowiązującego

Streszczenie

Cyberbezpieczeństwo jako przedmiot regulacji występuje w wielu aktach prawnych zarówno powszechnie obowiązujących, jak i wewnętrznych. Tego rodzaju regulacja znajduje się również w „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskie". Strategia ta jako akt prawa wewnętrznie obowiązującego ma ograniczoną moc. Ponieważ nie oddziałuje ona na podmioty zewnętrzne, nie może zatem stanowić podstawy indywidualnych rozstrzygnięć w stosunku do obywateli, przedsiębiorców i innych podmiotów. Jej podstawowy cel – podniesienie poziomu odporności na cyberzagrożenia – powinien stanowić priorytet polityki państwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, prawo wewnętrznie obowiązujące