Mirosław Karpiuk*

Cybersecurity as an element in the planning activities of public administration

Abstract

The focus of this article is on planning in the field of cybersecurity. Planning activities in this respect play a vital role, not only in systematising tasks relating to cybersecurity, but also of the authorities whose power extends to these matters. Cybersecurity occupies a special place in the public domain, and it is within this domain that planning is intended to ensure the coordination of activities in emergency situations. The plans which cover cybersecurity allow the prevention and monitoring of threats, and act accordingly as they arise, as well as to effectively remedy the effects caused by them.

Key words: cybersecurity, planning, public administration

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

Planning is one of the attributes of public administration. Therefore, its respective bodies, no matter whether they are based locally, or their scope of activity extends to the territory of the entire State, whether they are bodies of central – or local government administration, collegial or one-person bodies, they are obliged to prepare plans, strategies, and programmes of various kinds. In their planning documents, these bodies must sometimes plan for cybersecurity as an essential element which is intended to ensure the effective implementation of public tasks which require protection from cyber threats. Planning, including cybersecurity, facilitates the undertaking of coordinated tasks which allow the appropriate, timely, and harmonious fulfilment of the objectives of public administration in an organised and continuous manner, especially when engaging a number of entities.

A method characteristic of public law is based on the influence of public authorities on the recipients of the norms laid down by them, and on the enforcement of those norms[1]. The method might not always be applicable in the case of planning regulations. Some are not operative universally, so they do not affect external recipients, and the norms might not be enforceable. They include either guidelines for the legislator or patterns for acting in certain situations. The planning statutes pertaining to cybersecurity are often internally operative, so their scope is limited.

Cybersecurity is one of the tasks of both Government administration and local government, as well as other entities to which responsibility in this sphere has been delegated[2]. Cybersecurity, as an object of public activities, is also an aspect addressed in planning documents. It is defined as activities which are necessary to protect computer networks and systems, as well as the users of such systems, and other persons, from cyber threats[3]. Cybersecurity ensures the resistance of information systems to any activities which breach the confidentiality, integrity, accessibility, and authenticity of the data processed

1 I. Hoffman, *Jedynie teoretyczna możliwość wprowadzenia katastralnego systemu opodatkowania nieruchomości – uregulowania w zakresie podatków od nieruchomości na Węgrzech*, "Analizy i Studia" 2019, no. 2, p. 75.

2 K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021, p. 1, https://doi.org/10.4335/2021.5.

3 Article 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 (Cybersecurity Act) (OJ EU L 151, p. 15).

by them, or of related services provided by the systems[4]. It constitutes a specialised security division which is in charge of protecting information systems from threats[5].

The key planning document which directly addresses the issue of cybersecurity is The Cybersecurity Strategy of the Republic of Poland for the years 2019–2024 (hereinafter the strategy)[6]. Its primary objective is to improve resilience to cyber threats, and to increase the protection of information in the public, military, and private sectors, and to promote know-how and good practices, so that citizens' data are better protected. The strategy also formulates certain specific objectives: 1) the development of the national cybersecurity system; 2) an increase in the resilience of the information systems of the public administration and the private sector, and the improvement of the capabilities to effectively prevent and respond to incidents; 3) an increase in the national potential in terms of security in cyberspace; 4) building social awareness and expertise in cybersecurity; 5) building the strong international position of the Republic of Poland in the sphere of cybersecurity.

The development of the national cybersecurity system and the improvement of its effectiveness are to be attained, as set out in the strategy, by launching an information and communications system which supports 1) the cooperation of entities which are part of the national cybersecurity system; 2) generating and communicating recommendations concerning activities which improve cybersecurity; 3) reporting and responding to incidents; 4) risk assessment at the national level; and 5) cautioning against cyber threats. In this respect, it is important that Government administration and local government cooperate,

4 Article 2 (4) of the Act of 5 July 2018 on the National Cybersecurity System (i.e. Journal of Laws of 2002, item 1369 as amended). For more information on cybersecurity see M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, "Cybersecurity and Law" 2020, no. 2, pp. 57–72; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, "Cybersecurity and Law" 2020, no. 2, pp. 199–211; F. Radoniewicz [in:] red. W. Kitler, F. Radoniewicz, J. Taczkowska-Olszewska, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warsaw 2019, pp. 30–33; M. Karpiuk, *The organisation of the national system of cybersecurity. Selected issues*, "Studia Iuridica Lublinensia" 2021, no. 2.

5 M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, "Cybersecurity and Law" 2019, no. 2, p. 42.

6 The Cybersecurity Strategy of the Republic of Poland for the years 2019–2024 constitutes an annex to Resolution no. 125 on the Cybersecurity Strategy of the Republic of Poland for the years 2019–2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037).

in order, inter alia, to improve cybersecurity in local and regional structures, by creating secure networks and systems, and the possibilities of using them[7].

In connection with improving the resilience of the information systems of the public administration and the private sector, and building the capability to effectively prevent and respond to incidents, as laid down in the strategy, it is necessary to establish National Cybersecurity Standards as a set of organisational and technical requirements concerning, initially, the security of 1) apps, 2) mobile devices, 3) workstations, 4) servers and networks, 5) and cloud computing models.

In terms of expanding the national potential in cyberspace security, the strategy aims at investing in the development of industrial and technological resources for the needs of cybersecurity, by creating conditions for the growth of enterprises, and scientific and research institutes whose object of activity is to create solutions in the field of cybersecurity. One of the priorities is to improve the capabilities to design and manufacture software, devices, and services used in all sectors of industry in Poland, which contribute to its competitiveness.

The building of social awareness and expertise in cybersecurity is to be achieved, as set out in the strategy, by creating and implementing such a model of university education and professional improvement as will guarantee employee qualifications commensurate with the challenges. To that aim, model university-education curricula for cybersecurity courses of study must be prepared.

According to the strategy, in order to build the strong international position of the Republic of Poland in terms of cybersecurity, Poland must intensify its activities aimed at the security of the single digital market of the European Union, as the driving force behind economic growth and innovativeness. In addition, it is important that the strategy aims at including more aspects of cybersecurity in the work on the strengthening of the Common Foreign and Security Policy. The safety pillar of the Republic of Poland, and the pillar of the Euro-Atlantic security, lie in membership of the North Atlantic Treaty Organisation. Escalating hybrid attacks necessitate investing in the capacity

7 J. Kostrubiec, *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-Government in Poland*, "Lex Localis – Journal of Local Self-Government" 2021, no. 19(1), p. 126, https://doi.org/10.4335/19.1.111-129(2021).

to deter and protect, and to improve the resilience and capability to react quickly and effectively to cyber attacks.

As far as cybersecurity is concerned, it is proposed, in planning documents, to improve resilience to cyber threats and the protection of information in the public, military and private sectors, as well as to promote know-how and good practices so that citizens' data are better protected. In this respect the aim should be 1) to improve the resilience of information systems used in the public, private, military, and civilian spheres, and to attain the capability to effectively prevent, fight, and respond to cyber threats; 2) to improve the defensive potential of the State by guaranteeing the continuous development of the national cybersecurity system; 3) to build the capabilities to carry out the whole range of military activities in cyberspace; 4) to develop national capabilities to test, examine, evaluate, and certify solutions and services in the field of cybersecurity; 5) to develop abilities, knowledge, and awareness of threats and challenges among public administration staff, and among the public in the field of cybersecurity; and 6) to boost and develop the State's potential by, for example, developing home-made solutions in the field of cybersecurity, and conducting research and development, financed by the State, in the sphere of modern technologies, teaching machine learning, the Internet of Things, and stationary and mobile broadband networks (5G and newer generation), also including cooperation with universities, scientific institutions, and enterprises, in both the public and private sectors[8].

Ensuring the safe functioning of the State and citizens in the information space is also highlighted. To achieve this aim it is necessary 1) at the strategic level, to build the capabilities to protect the information space (to systemically fight misinformation), understood as permeating layers of the spaces: virtual (the layer of systems, software, and apps), physical (infrastructure and hardware), and cognitive; 2) to create a uniform system of the State's strategic communication aimed at predicting, planning, and carrying out cohesive communication tasks, using a wide range of communication channels and media, making use of recognition and interaction tools in various spheres of national

8 The National Security Strategy of the Republic of Poland, Warsaw 2020, p. 20. The President of the Republic of Poland, who safeguards the sovereignty and security of the State and the integrity and inviolability of its territory, approves of, at the request of the Prime Minister, the national security strategy, Article 4a (1) (1) of the Act of 21 November 1967 on the General Defence Obligation of the Republic of Poland (i.e. Journal of Laws of 2021, item 372, as amended).

security; 3) to actively prevent misinformation by building the capabilities and creating procedures of cooperation with information and social media, with involvement on the part of citizens and non-governmental organisations; 4) to aim at raising social awareness of threats connected with information manipulation, through education in the field of information security[9].

Descriptions of threats and assessments of the risk of those threats, including those such as disruption to the operation of information networks and systems, are included in the National Crisis Management Plan. This kind of disruption is caused by cyber threats, and includes both intentional actions (attacks, sabotage), making use of information systems, and the actions targetted at information systems and in cyberspace, as well as unintentional acts (breakdowns, errors). They are among the most burdensome (in terms of damage) incidents which strike at contemporary society. Incidents involving computer systems and cyberspace are becoming more and more common, because 1) the only device needed to launch an attack or sabotage in cyberspace is a computer with a network connection; 2) cyberspace does not have any control barriers. Attackers create viruses, worms (Trojan horses) and send them to the target place of attack, and undertake activities aimed at destroying servers, modifying computer systems, and falsifying websites; 3) the probability of finding gaps in security mechanisms is relatively high, and the targets of intentional actions are very diverse – computer networks, Government computers, systems of banks, enterprises and individual users, are at risk; and 4) the commonness of using computer systems and the variety of those systems result in the higher and higher probability of failures and errors resulting in incidents[10]. The causes of these threats are 1) the human factor, 2) computer sabotage and lack of supervision, 3) the modification of systems and data, 4) technical or programming errors (the vulnerability of apps), and 5) failure, damage, or theft of transmission elements. Cyber threats include 1) to institutions and State offices, and other organisational units, as well as local government units; 2) to entrepreneurs, including operators of critical infrastructure; and 3) cross-border incidents from outside the territory of a State. The most frequent effects of cyber threats are 1) the loss of trust in public institutions; 2) the inability to carry out tasks by employees; 3) the inability to obtain, communicate, and share information;

9 Ibidem, p. 21.

10 See also F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warsaw 2016, pp. 128–129.

4) the risk of the loss of life and health caused by disruptions to power and traffic-control systems; 5) the limitation of the possibilities to inform the public about upcoming threats; 6) breaches of the security of the State and its citizens; 7) breakdowns of systems or the malfunctioning of equipment or software; 8) the occurrence of threats to the State's defence; 9) disruptions to the operation of the transmission infrastructure; 10) reduced supplies of energy and fuel, limited provision of banking and financial services, food and water, healthcare, transport, communication and emergency services, and the functioning of public administration bodies; 11) disruptions to the functioning of telecommunications and communications systems; 12) significant financial and economic losses, as well as social consequences, changes or disturbances to processes – the violation of integrity[11].

In partial reports which are used for preparing a dossier on threats to national security (drawn up for the needs of the National Crisis Management Plan), there are pointed out the most significant threats, and the effects of their occurrence, by creating a risk map, covering the types and characteristics of these threats, including cybersecurity threats which might lead to a crisis[12].

Bibliography

Literature

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, "Cybersecurity and Law" 2019, no. 2.

Hoffman I., Cseh K.B., *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, "Cybersecurity and Law" 2020, no. 2.

Hoffman I., *Jedynie teoretyczna możliwość wprowadzenia katastralnego systemu opodatkowania nieruchomości – uregulowania w zakresie podatków od nieruchomości na Węgrzech*, "Analizy i Studia" 2019, no. 2.

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

Karpiuk M., *The organisation of the national system of cybersecurity. Selected issues*, "Studia Iuridica Lublinensia" 2021, no. 2.

Kostrubiec J., *The Role of Public Order Regulations as Acts of Local Law in the Performance of Tasks in the Field of Public Security by Local Self-Government in Poland*, "Lex Localis – Journal of Local Self-Government" 2021, no. 19(1).

11 *National Crisis Management Plan. The 2020 Revision. Part A*, https://rcb.gov.pl/wp-content/uploads/KPZK-cz.-A-2020-1-1.pdf.

12 § 3 (1) (e) of the Ordinance /Regulation of the Council of Ministers of 11 December 2020 on the Report on Threats to National Security (Journal of Laws, item 2344).

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warsaw 2016.
Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, red. W. Kitler, F. Radoniewicz, J. Taczkowska-Olszewska, Warsaw 2019.

Normative Acts

Act of 21 November 1967 on the General Defence Obligation of the Republic of Poland (i.e. Journal of Laws of 2021, item 372, as amended).
Act of 5 July 2018 on the National Cybersecurity System (i.e. Journal of Laws of 2002, item 1369 as amended).
National Crisis Management Plan. The 2020 Revision. Part A, https://rcb.gov.pl/wp-content/uploads/KPZK-cz.-A-2020-1-1.pdf.
Ordinance/Regulation of the Council of Ministers of 11 December 2020 on the Report on Threats to National Security (Journal of Laws, item 2344).
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 (Cybersecurity Act) (OJ EU L 151, p. 15).
The Cybersecurity Strategy of the Republic of Poland for the years 2019–2024 constitutes an annex to Resolution no. 125 on the Cybersecurity Strategy of the Republic of Poland for the years 2019–2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037).
The National Security Strategy of the Republic of Poland, Warsaw 2020.

Cyberbezpieczeństwo jako element działalności planistycznej administracji publicznej

Streszczenie

Problematyka artykułu dotyczy planowania w przestrzeni cyberbezpieczeństwa. Działalność planistyczna w tym zakresie pełni ważną rolę, porządkuje nie tylko zadania dotyczące cyberbezpieczeństwa, ale też organy właściwe w tych sprawach. Szczególne miejsce cyberbezpieczeństwo zajmuje w przestrzeni publicznej i to właśnie w jej ramach planowanie ma zapewnić koordynację działań w sytuacjach zagrożenia. Plany obejmujące sferę cyberbezpieczeństwa pozwalają na przeciwdziałanie zagrożeniom, monitorowanie ich, właściwe zachowanie się w przypadku ich wystąpienia, a także na sprawne usuwanie skutków przez nie wywołanych.

Słowa kluczowe: cyberbezpieczeństwo, planowanie, administracja publiczna