Mirosław Karpiuk*

The executive agency as a legal organisational form of implementing cybersecurity tasks

Abstract

The national cybersecurity system is formed of a number of public entities, including executive agencies with legal personality as entities of the public finance sector. The executive agency could implement cybersecurity tasks important to the functioning of the state and its institutions. Through this legal organisational form, it would be possible to shape the development of new technologies that could then serve a digital society or digital state, including the protection of ICT systems for communication, as well as the provision of digital services and key services. Due to the widespread activity in cyberspace, it is necessary to have entities in place to protect its users. Such an entity could have the form of a cyber agency, working with other institutions (public and private), that is competent for cybersecurity.

Key words: cybersecurity, cyberspace, executive agency

* 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.

Introduction

There is a clear realisation that the development of new technologies, both civilian and military ones, contributes to a significant increase in the employment of unmanned and autonomous systems, automated and robotised weapon platforms using artificial intelligence, as well as long-range precision weapon systems. Digital technologies are advancing rapidly, and the development of solutions based on fixed line and mobile broadband, the Internet of Things, cloud computing, quantum technologies, automation of services, nanotechnology and artificial intelligence creates new development opportunities for Poland, while also generating previously unknown threats. The challenge for the state consists in joining the technological race in this area, which would offer Poland the opportunity to overcome the position of a mere user and join a group of countries with effectively functioning digital economies, providing solutions and co-creating international standards. It should be stated that communication systems are a key component of national security assets and preparatory measures for crisis situations, so they constitute an important element of the national critical infrastructure. In this respect, a key challenge is to develop secure and modern telecommunications networks capable of handling the increasing number of end users and systems. In the context of the digital revolution, the specific roles of cyberspace and information space should be taken into account. This also creates room for disinformation and the manipulation of information, which requires effective strategic communication activities[1].

Social and economic development is more and more dependent on fast and unhindered access to information and its use in management, production, services and the public sector. The dynamic progress of information systems serves the national economy. The use of digital technologies that comprise cyberspace affects the formation of social relationships, and online services have become a tool for influencing the behaviour of social groups, as well as a means of exerting political influence[2].

Ensuring digital security is one of the primary tasks of state authorities. Threats of an IT nature have increasingly serious consequences, and

1 *National Security Strategy of the Republic of Poland*, Warszawa 2020, p. 7–8.

2 Cybersecurity Strategy of the Republic of Poland – 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 Republic of Poland 2019, item 1037).

cyberattacks can be used as a means of economic as well as political pressure[3]. The executive cyber agency could play its part in ensuring digital security, which may additionally support the development of new technologies that could also be used to ensure this security.

Cybersecurity, defined as the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[4], could also be the spectrum of an executive agency set up for this purpose, especially in an era where cyberattacks are not only more and more frequent, but also carry more and more consequences. Since information systems are now the basis of many areas of public, private, or social activity, or are an instrument supporting or greatly facilitating such activity, they must not only develop rapidly, but must also be properly protected. Such tasks can be given to the cyber agency.

The place of the cyber agency in the national cybersecurity system

Pursuant to Art. 3 of the NCSA, the objective of the national cybersecurity system is to ensure cybersecurity at the national level, including the uninterrupted provision of essential services and digital services by achieving an appropriate level of security for the information systems used to provide these services, and ensuring the handling of incidents[5]. The executive agency,

3 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 145.

4 Art. 2(4) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws 2020, item 1369, as amended) – hereinafter referred to as the NCSA For more information about cybersecurity refer to: M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, ibidem 2019, no. 2; M. Karpiuk, *Activities of the local government units in the field of telecommunications*, ibidem, no. 1; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; 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; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2.

5 See also: I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1, p. 175.

as an entity of the public finance sector, will also be among the entities included in the national cybersecurity system, as provided for by Art. 4(7) of the NCSA. It will therefore be obliged to ensure that information systems are protected in such a way as to allow the uninterrupted provision of essential services and digital services.

The executive agency is therefore a public-finance sector entity. At the same time, it should be emphasised that separating the public finance sector makes it easier to draw the circle of entities obliged to apply certain universal principles of financial management specific to public sector entities[6].

Legal organisational form

The executive agency can serve as one of the legal organisational forms through which to perform cybersecurity tasks. This form has already become a permanent fixture in the Polish political and legal space. Not only is it recognisable, but its mechanisms are already proven on many levels of operation, so there is a high probability that in the realm of cybersecurity it can properly fulfil the tasks assigned to it.

Cybersecurity matters in the military dimension fall within the competency of the Minister of National Defence, while cybersecurity in the civilian dimension is the responsibility of the minister competent for computerisation[7]. Depending on the status of such an agency, one of these ministers would supervise its activities.

Executive agencies are regarded as the new management governance instrument, which is defined as the orientation of public administration to achieve specific results through the implementation of specific tasks, which should be verified on the basis of measurable standards or indicators. In this perspective, the public administration becomes responsible for the efficient provision of services[8]. The executive agency could therefore work effectively in cyberspace, in terms of both developing new cyber technologies and

6 M. Cilak [in:] *Ustawa o finansach publicznych. Komentarz*, ed. Z. Ofiarski, Warszawa 2020, art. 9.

7 Art. 12a and 19 of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended). See also M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1, p. 86–87.

8 K. Marchewka-Bartkowiak, *Agencje wykonawcze*, „Infos" 2011, no. 19, p. 1.

countering cyber threats. Innovation is the spectrum of activities that the executive agency can successfully deal with. Its rules would have to be detailed in the statute.

The executive agency is a state-owned legal entity formed under statutory law to carry out the state's tasks[9]. The solutions adopted for executive agencies by the Polish legislator were modelled on EU legislation[10].

Organisational structure

The organisational structure of the cyber agency can be mapped to already existing executive agencies dealing with other issues. Certain legal solutions for the organisational structure could be borrowed from the statutory solutions adopted, for example, from the Military Property Agency[11], applying them to the cyber agency, accordingly, while taking into account the specifics of its activities.

Thus, the cyber agency would be an executive agency within the meaning of the APF, supervised by the Minister of National Defence or the minister competent for computerisation (depending on the scope of its activities – cybersecurity in the military dimension or cybersecurity in the civilian dimension). It would operate on the basis of statutory law and the statute. It would consist of: 1) the Office of the Head of the Cyber Agency; 2) regional branches (if formed). The Minister of National Defence or alternatively, the minister competent for computerisation (competent minister), by way of regulation, would determine the statute of the cyber agency, specifying its internal organisation, including a list of managerial positions in the Office of the Head of the Cyber Agency, as well as a list of regional branches, and their the substantive and local jurisdiction, taking into account the need to ensure the efficient performance of the agency's tasks. The cyber agency bodies could be: 1) the Head of the Cyber Agency; 2) the Supervisory Board; 3) directors of regional branches (if formed).

9 Art. 18 of the Act of 27 August 2009 on Public Finance (consolidated text, Journal of Laws 2021, item 305, as amended), hereinafter the APF.

10 See Council Regulation (EC) no. 58/2003 of 19 December 2002 laying down the statute for executive agencies to be entrusted with certain tasks in the management of Community programmes (Official Journal of the European Union 2003, L 11, p. 1).

11 The Act of 10 July 2015 on the Military Property Agency (consolidated text, Journal of Laws 2021, item 303, as amended).

The Head of the Cyber Agency would be appointed and dismissed by the President of the Council of Ministers on the proposal of the competent minister. Appointment to the role would mean the establishment of an employment relationship. The term of office would last three years. The term of office of the Head of the Cyber Agency would expire upon: 1) his death; 2) resignation; 3) dismissal. After the expiration of the term of office of the Head of the Cyber Agency for the reasons specified above, his duties would be performed by his deputy designated by the competent minister, until the new Head of the Cyber Agency assumes his duties. The position of the Head of the Cyber Agency could be held by a person who: 1) has a master's degree or equivalent; 2) is a Polish citizen; 3) enjoys full public rights; 4) has not been validly sentenced for an intentional crime or an intentional fiscal crime; 5) has managerial competence; 6) has at least six years of work experience, including at least three years of work experience in a managerial position; 7) has education and knowledge related to matters falling within the competency of such an agency.

The Head of the Cyber Agency would act with the assistance of not more than four deputies and directors of regional branches (if formed). Deputies of the Head of the Cyber Agency would be appointed and dismissed by the competent minister upon the proposal of the Head of the Cyber Agency. Executive positions in the Office of the Head of the Cyber Agency would be appointed and dismissed by the Head of the Cyber Agency. These appointments would imply the establishment of an employment relationship within the meaning of the Labour Code.

The cyber agency's regional branches would be formed for the area of one or more provinces or parts thereof. Regional branches would be managed by directors with the help of deputies. The cyber agency's regional branch directors and their deputies would be appointed and dismissed by the Head of the Cyber Agency. Appointment to these roles would mean the establishment of an employment relationship.

In civil cases the cyber agency would be represented before courts by the Head of the Cyber Agency and by regional branch directors having the substantive and local jurisdiction. In labour law cases the cyber agency would be represented before courts by the Head of the Cyber Agency with respect to employees working in the Office of the Head of the Cyber Agency and by competent directors of the regional branches, having substantive and local jurisdiction, with respect to employees working in the regional branches.

The Supervisory Board would consist of seven members appointed by the relevant minister in consultation with the minister competent for public

finance. The relevant minister, in consultation with the minister competent for public finance, could dismiss the Supervisory Board or its individual members during the term of office. In the case of dismissal of a member of the Supervisory Board, a new member would be appointed for the remainder of the ongoing term of office of the Supervisory Board. The Supervisory Board would be composed of five representatives of the relevanrt minister and two representatives of the minister competent for public finance. The chairman of the Supervisory Board would be appointed for the term of office by the relevant minister from among the members of the Supervisory Board. The relevant minister could dismiss the Chairman of the Supervisory Board during his term of office at any time. Removal from this office would not mean removal from the Supervisory Board. The term of office of the Supervisory Board would be three years. The term of office of a member of the Supervisory Board would expire upon: 1) his death; 2) resignation; 3) dismissal. The Supervisory Board would exercise permanent supervision over the cyber agency's activities.

Financial economy

The basis of the executive agency's financial economy (as is clear from Art. 21 of the APF) is an annual financial plan comprising of: 1) revenue; 2) subsidies from the state budget; 3) a statement of the operational costs of the executive agency, as well as the costs of performing statutory tasks, distinguishing the costs of having other entities perform these tasks – specifying salaries and contributions calculated on them, payments of interest arising from incurred liabilities and the purchase of goods and services; 4) the financial result; 5) funds for capital expenditures; 6) funds allocated to other entities; 7) the balance of receivables and liabilities at the beginning and end of the year; 8) the balance of cash at the beginning and end of the year. The annual financial plan of the executive agency is drafted by its competent authority in consultation with the minister exercising supervision over the executive agency. After approval by the minister exercising supervision, the draft is forwarded to the Minister of Finance. Within the framework of the draft financial plan, a plan of revenue and expenditures of the executive agency recognised on the date of their payment is drawn up, and in this plan of revenue and expenditures, the planned expenditures should not be higher than the planned revenues. Planned expenditures may exceed planned revenue in exceptional instances, but only with the approval of the minister supervising

the executive agency, issued in consultation with the Minister of Finance. The financial plan of the executive agency may be amended in terms of revenue and expenses after obtaining the approval of the minister exercising supervision over the agency, which is issued after obtaining the opinion of the parliamentary committee responsible for the budget. The Minister of Finance must be notified immediately of any amendments made. As a rule, amendments to the executive agency's financial plan may not result in an increase in the agency's liabilities or worsen the agency's projected financial result. The executive agency may receive subsidies from the state budget, to the extent specified in statutory law under which it is formed. It may incur obligations for the period of performance of a given task exceeding the budgetary year, if the expenses necessary to service the debt are recognised in the annual financial plan.

Financial plans of executive agencies are also included in annexes to the state budget act as required under Art. 122(1)(1)(a) of the APF The financial plans of executive agencies, annexed to the state budget act, are of special character, thus due to their nature and subject matter they cannot be directly included in the state budget. They cannot be mechanically or accountably attached to the state budget, they must function separately[12].

The statutorily guaranteed minimum level of detail of the executive agency's financial plan is a manifestation of openness in the management of public funds. The regulations also provide for a special procedure for determining the executive agency's financial plan, which involves cooperation and supervision by various bodies. It consists in delegating authority in this regard to the competent authority, acting in consultation with the minister exercising supervision over the executive agency. The draft version of the financial plan is subject to approval by the minister exercising supervision[13].

The executive agency's financial economy rules are quite rigid in nature. It is not permitted, without an amendment to the state budget act in the part being an annex containing the financial plan of a given executive agency, to change its financial plan, which consists in a simultaneous increase in its own revenues and costs of performing its tasks, since the above amounts are presented in the state budget act[14].

However, the disadvantage of such an agency is the obligation to pay surplus funds into the state budget. Such rules for the settlement of surplus

12 A. Borodo [in:] *Ustawa o finansach*..., art. 122.
13 L. Lipiec-Warzecha, *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011, art. 21.
14 K. Kopyściańska [in:] *Ustawa o finansach*..., art. 21.

funds are laid down in Art. 22 of the APF Thus, the executive agency is obliged to pay annually to the state budget, to the account of the revenues of the state budgetary unit serving the minister supervising the agency, the surplus of the funds, determined at the end of the year, which remains after settling tax liabilities. This surplus shall be transferred by the executive agency as soon as the liabilities due from the reporting period are settled, but no later than on 30 June of the year following the year in which the surplus arose. In particular, justified cases arising from the need to ensure the efficient and full performance of the tasks of the executive agency, the Council of Ministers may, at the request of the minister exercising supervision over the executive agency, agree, by resolution, not to pay surplus funds into the state budget. The Minister exercising supervision over the executive agency, in consultation with the Minister of Finance, shall decide, by way of regulation, the method of determining the surplus, having regard for the need to ensure continuity of funding for the Agency's tasks, making investments necessary for the performance of state tasks, and taking into account the funding sources for the tasks carried out by the agency. Such regulation would also have to be issued with respect to the executive cyber agency.

Therefore, the regulation should specify how to determine the surplus of the cyber agency's funds that are subject to payment into the state budget. The surplus of the agency's funds shall be determined by taking into account the income received from sources other than the state budget and the expenses incurred by the cyber agency, with the exception of expenses for the performance of the tasks for which the agency received funds from the state budget. Furthermore, the surplus of the agency's funds shall be determined by taking into account the funds deposited in bank accounts at the end of the budgetary year, except for: 1) dividends; 2) unused funds from reimbursable grants, funds from the budget of the European Union and non-reimbursable funds from aid provided by member states of the European Free Trade Agreement (EFTA); 3) restricted funds: (a) of the employee benefit fund and the repair & renovation fund, (b) bid securities, (c) guarantee deposits and performance bonds, (d) prepayments made by the agency's contractors deposited in the agency's bank accounts at the end of a given budgetary year, including prepayments made to the agency as part of the implementation of tasks in the area of national defence and state security, (e) overpayments and erroneous payments made by the agency's contractors, (f) funds deposited in the VAT account. When determining the surplus of funds, the funds to be settled shall be reduced by the tax liabilities determined at the end of the budgetary

year, or liabilities due by 31 March of the following year, excluding liabilities related to funds not taken into account when determining the surplus[15].

All executive agencies are required to pay annually to the state budget any surplus funds obtained as a result of their activities, and payments of these surplus funds should be classified as a type of untaxed revenue of the state budget[16]. Executive agencies, being unable to keep surplus funds for themselves, should not thereby be incentivised to achieve a surplus[17].

The cyber agency should receive an operating subsidy from the portion of the state budget administered by the Minister of National Defence if the funds planned to be earned from operations would not be sufficient enough to cover operational costs. It should also receive an earmarked subsidy from the portion of the state budget administered by the Minister of National Defence for carrying out certain assigned tasks.

Financial support for cyber agencies could also be provided through the Cyber Security Fund. Its statutory objective is to support efforts to ensure that communication and information systems are guaranteed protection against cyber threats. This is an earmarked state fund, the administrator of which, in the current state of law, is the minister competent for computerisation[18]. Since the Cyber Security Fund currently makes payments of telecommunications benefits, subsidising other areas of activity would require an amendment to statutory law.

Attention should be paid to the transparency and integrity of the executive agency's management, especially in terms of financial management, which determines the need to implement internal control procedures, as well as to define a clear mechanism for external control of its activities.

15 Cf. § 1–3 of the Regulation of the Minister of National Defence dated 24 October 2017 on Determining Surplus Funds of the Military Property Agency (consolidated text, Journal of Laws 2019, item 2299).

16 K. Kopyściańska [in:] *Ustawa o finansach*…, art. 22.

17 C. Kosikowski, *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011, art. 22.

18 Art. 2 of the Act of 2 December 2021 on Special Rules of Remuneration for Persons Performing Cybersecurity Tasks (Journal of Laws 2021, item 2333, as amended). See also M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Conclusions

The legal organisational form of the executive agency can be used to perform public tasks that are important for the functioning of the state, including its (cyber) security. Based on the example of EU solutions, as well as those adopted in Poland, it can be seen that executive agencies perform tasks mostly in areas such as research and development, or new technologies, and therefore could (effectively, it seems) perform the tasks arising from the sphere of cybersecurity. The cyber agency could be a non-commercial business-support institution, which can positively influence not only the development of the business environment, but also the development of the region in which such an agency is based or operates. It could also establish cooperation with various entities from both the public and private sectors, as well as the social sector, depending on the projects being implemented.

The cyber agency's objectives must correspond to the strategic objectives defined in both the Security Strategy of the Republic of Poland and the Cybersecurity Strategy of the Republic of Poland. These include: 1) enhancing resilience to cyber threats and increasing the level of protection of information in both the civilian and military sectors, as well as promoting knowledge and good practices to better protect information; 2) developing the national cybersecurity system using private and public capabilities; 3) enhancing resilience of information systems and achieving the ability to effectively prevent and respond to incidents; 4) enhancing national cybersecurity capabilities; 5) building public awareness and competence in the field of cybersecurity; 6) building a strong international position of the Republic of Poland in the area of cybersecurity; 7) enhancing the resilience of information systems used in the military sphere and achieving the ability to effectively prevent, combat, and respond to cyber threats; 8) strengthening the defensive capabilities of the state by ensuring the continued development of the national cybersecurity system; 9) achieving the ability to conduct a wide range of military and non-military activities in cyberspace; 10) developing national capabilities in the area of testing, research and the evaluation of cybersecurity solutions and services; 11) developing competence, knowledge and the awareness of threats and challenges among public administration personnel and society in the area of cybersecurity; 12) strengthening and expanding the capabilities of the state through the development of indigenous solutions in the area of cybersecurity and conducting state-funded research and development in the area of modern technologies, among others; 13) establishing cooperation,

including universities and scientific institutions and companies, both in the public and private sector; 14) enhancing the cybersecurity of essential and digital services, as well as of critical infrastructure; 15) expanding industrial and technological resources for the purposes of cybersecurity in the military dimension[19].

Bibliography

Chałubińska-Jentkiewicz K., Karpiuk M., Kostrubiec J., *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021.
Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.
Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.
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., 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., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Activities of the local government units in the field of telecommunications*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.
Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.
Kosikowski C., *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011.
Lipiec-Warzecha L., *Ustawa o finansach publicznych. Komentarz*, Warszawa 2011.
Marchewka-Bartkowiak K., *Agencje wykonawcze*, „Infos" 2011, no. 19.
National Security Strategy of the Republic of Poland, Warszawa 2020.
Ustawa o finansach publicznych. Komentarz, ed. Z. Ofiarski, Warszawa 2020.

19 See also M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, ibidem 2021, no. 1, p. 47–50.

Agencja wykonawcza jako forma organizacyjno-prawna realizacji zadań ze sfery cyberbezpieczeństwa

Streszczenie

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów publicznych, w tym posiadające osobowość prawną agencje wykonawcze będące jednostkami sektora finansów publicznych. Agencja wykonawcza mogłaby również realizować zadania z dziedziny cyberbezpieczeństwa, jako ważne z punktu widzenia funkcjonowania państwa i jego instytucji. Za pośrednictwem tej formy organizacyjno-prawnej można byłoby kształtować rozwój nowych technologii, które mogłyby następnie służyć cyfrowemu społeczeństwu czy też cyfrowemu państwu, w tym chronić systemy teleinformatyczne służące komunikowaniu się, a także świadczeniu usług cyfrowych i usług kluczowych. Ze względu na powszechną aktywność w cyberprzestrzeni muszą istnieć podmioty, które będą chronić jej użytkowników. Takim podmiotem może być cyberagencja współpracująca z innymi instytucjami (publicznymi i prywatnymi), właściwa w sprawach cyberbezpieczeństwa.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, agencja wykonawcza