Mirosław Karpiuk*

Tasks of the Minister of National Defense in the area of cybersecurity

Abstract

The Minister of National Defense, as an organ of government administration whose jurisdiction also extends to cybersecurity in the military dimension, has been provided by the legislator with specific measures to ensure cybersecurity in the Armed Forces of the Republic of Poland, or in the units subordinate to them or supervised by them – in the military dimension. The Minister of Defense is in charge of the Computer Security Incident Response Team operating at the national level, through which they also perform tasks related to information systems security.

Key words: cybersecurity, Minister of National Defense, Polish Armed Forces

* 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.

In peacetime, the President of the Republic of Poland exercises authority over the Armed Forces through the Minister of National Defense[1]. In peacetime, authority is exercised with civilian control of the military[2].

The Minister of National Defense, as the chief agency of government administration that is competent in the field of national defense, has been equipped by the legislator with specific tasks and competences concerning this sphere, both during the normal functioning of the state and during threats, including threats of a qualified nature. Their role in providing military security is very important[3].

Ensuring digital security is one of the key tasks of state authorities. The functioning of the information society relies on information and communication networks and systems, but these are susceptible to disruptions that affect their operation. Threats to the information technology side of society's functioning have increasingly serious consequences, and cyberattacks can be used as a means of economic and political pressure[4].

Cybersecurity, defined by the legislator as the resistance of information systems to actions that violate the confidentiality, integrity, availability, and authenticity of the processed data or related services offered by these systems[5] is the sphere that certain public administration agencies are obliged to protect, including the Minister of National Defense.

The national defense department, which is headed by the Minister of National Defense, covers the following matters in peacetime: 1) national defense and the Armed Forces of the Republic of Poland; 2) cybersecurity in

1 Art. 134 sec. 2 of the Constitution of Poland dated April 2, 1997 (Journal of Laws of 1997 no. 78 item 483 as amended). See also: M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3, p. 392; P. Winczorek, *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008, p. 292. The President of the Republic of Poland cannot implement independent policy in matters related to the functioning of the Armed Forces of the Republic of Poland, B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2009, p. 666–667.

2 W. Skrzydło, *Komentarz do art. 134* [in:] idem, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.

3 M. Karpiuk, *Zadania i kompetencje Ministra Obrony Narodowej w czasie stanów nadzwyczajnych – ujęcie normatywne* [in:] *Minister Obrony Narodowej i Naczelny Dowódca Sił Zbrojnych w systemie kierowania bezpieczeństwem narodowym RP. Wybrane problemy*, ed. W. Kitler, Warszawa 2013, p. 93.

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

5 Art. 2 item 4 of the Act dated July 5, 2018 on the National Cybersecurity System (consolidated text Journal of Laws of 2020, item 1369, as amended).

the military dimension; 3) participation of the Republic of Poland in military undertakings of international organizations and within the scope of fulfilling its military obligations arising from international agreements; 4) offset agreements – unless, under separate provisions, specific issues belong to the scope of tasks and competencies of the President of the Republic of Poland or other state agencies[6]. The jurisdiction of the Minister of Defense, therefore, includes cybersecurity matters only in the military dimension. Civilian cybersecurity matters are covered by the Information Technology department.

The scope of responsibilities of the Minister of National Defense includes directing, in peacetime, all activities of the Armed Forces of the Republic of Poland[7], and in the area of preparing national defense assumptions, in particular, collecting information and conducting analyses and developing forecasts about the formation of the conditions of national security, as well as formulating proposals for the Council of Ministers and other state agencies relating to defense policy[8]. Peacetime management of all activities of the Armed Forces of the Republic of Poland also concerns cyberspace security; matters in this area also fall within the scope of defense policy.

The Minister of Defense is responsible for: 1) cooperation of the Polish Armed Forces with the competent agencies of the North Atlantic Treaty Organization, the European Union and international organizations in the area of national defense in the field of cybersecurity; 2) ensuring the ability of the Polish Armed Forces in the national, allied, and coalition system to conduct military operations in the event of a cybersecurity threat necessitating defensive measures 3) developing the cybersecurity assurance capabilities of the Polish Armed Forces by organizing specialized training events; 4) acquiring and developing tools to build cybersecurity assurance capabilities in the Polish Armed Forces; 5) overseeing activities related to incident handling during martial law[9]; 6) assessing the impact of incidents on the state defense

6 Art. 19 sec. 1 of the Act of September 4, 1997 on departments of government administration (i.e. Journal of Laws of 2021, item 1893, as amended).

7 Art. 2 item 1 of the Act of December 14, 1995 on the Office of the Minister of National Defense (i.e. Journal of Laws of 2019, item 196).

8 Para. 1 item 1 (a) of the Regulation of the Council of Ministers of July 9, 1996 on the detailed scope of activities of the Minister of National Defense (Journal of Laws of 1996, no. 94, item 426, as amended).

9 In the event of an external threat to the state, including that caused by acts of a terrorist nature or acts in cyberspace, an armed attack on the territory of the Republic of Poland, or where an international agreement imposes an obligation to defend the country jointly against aggression, the President of the Republic of Poland may, at the request

system; 7) assessing cybersecurity threats during martial law and presenting proposals for defense operations to the relevant authorities; 8) coordinating, in cooperation with the minister in charge of internal affairs and the minister in charge of information technology, the execution of tasks of government administration agencies and local government units during martial law concerning defense operations in the event of a cybersecurity threat. This liability arises under Art. 51 of the Act on the National Cybersecurity System.

The Minister of Defense performs their tasks directly and through plenipotentiaries and coordinators appointed by decision[10]. In exercising this authority, they have appointed their plenipotentiary for cybersecurity whose duties include: 1) issuing guidelines on behalf of the Minister of National Defense in cyberspace security matters with regard to units and organizational entities of the national defense department, excluding tasks reserved for classified information protection plenipotentiaries; 2) initiating and supporting activities of units and organizational entities of the national defense department in the area of achieving the capability to ensure cyberspace security of the department; 3) overseeing the implementation of tasks resulting from legal acts, policies, and government programs related to ensuring cyberspace security of the department of national defense; 4) taking actions to promote a consistent, uniform, and effective cyberspace security management system of the department of national defense; 5) representation of the national defense department in the works of the leading bodies (committees, teams, groups) of the North Atlantic Treaty Organization and the European Union in the area of cyberspace security; 6) cooperation with

of the Council of Ministers, impose martial law in some or all of the country's territory. Cyberspace is understood as the space for processing and exchange of information created by information and communications technology systems, together with the links between them and relations with users, Art. 2 of the Act of August 29, 2002 on martial law and on the competences of the Commander-in-Chief of the Armed Forces and the principles of their subordination to the constitutional bodies of the Republic of Poland (consolidated text of the Journal of Laws of 2017, item 1932). See also: K. Chałubińska-Jentkiewicz, A. Brzostek, *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021, p. 13. Actions in cyberspace may therefore be grounds for introducing martial law.

10 Para. 5 sec. 2 item 3 of the organizational regulations of the Ministry of National Defense constituting an annex to order no. 33/MON of the Minister of National Defense of August 24, 2015 on the organizational regulations of the Ministry of National Defense (Official Gazette of the Ministry of National Defense of 2015, item 250, as amended).

expert teams of the national defense department performing tasks in the area of cyberspace security[11].

The Plenipotentiary of the Minister of National Defense for Cybersecurity under § 2 sec. 2 of the decision may in particular: 1) request the presentation of positions, information, documents, and reports periodically or concerning particular matters or types of matters to the appropriate substructures and organizational units of the national defense department; 2) make assessments and formulate conclusions in the implementation of cybersecurity activities; 3) commission research, analysis, and expertise in the scope of its tasks.

The Plenipotentiary of the Minister of Defense for Cyberspace Security may undertake cooperation with public administration agencies and non-governmental organizations as well as national and international entities performing tasks related to cyberspace security. These powers are derived from § 4 of the decision. Collaboration can involve both state and local government but can only include cybersecurity tasks.

Government administration agencies responsible for cybersecurity issues are, in particular, ministers in charge of specific branches of government administration, as well as the Financial Supervision Commission[12]; cybersecurity issues are also handled by local government agencies[13].

The Minister of National Defense maintains the National Contact Point for Cooperation with the North Atlantic Treaty Organization, whose tasks, according to Art. 52 of the Act on the National Cybersecurity System, include:

11 Para. 1–2 sec. 1 of decision No. 14/MON of the Minister of National Defense of January 25, 2019 on the appointment of the Plenipotentiary of the Minister of Defense for Cybersecurity (Official Gazette of the Ministry of National Defense of 2019, item 19 as amended), hereinafter the decision.

12 For more information on the status of the Financial Supervision Commission in the cybersecurity sphere, see: P. Pelc, *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, no. 2, p. 193–195; K. Dygasiewicz, P. Zapadka, *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej społecznościowej w czasach gospodarki COVID lub postCOVID, w świetle Komunikatu Komisji Nadzoru Finansowego*, ibidem, no. 1, p. 103–112; P. Pelc, *The COVID-19 pandemic and the functioning of financial institutions in Poland*, ibidem, p. 101; idem, *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, ibidem 2021, no. 1, p. 39-40.

13 For more information on the status of local government in the cybersecurity sphere, see: 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. 39–57; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, ibidem, no. 1, p. 37–45; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity for the municipalities in Hungary*, ibidem 2020, no. 2, p. 199–210.

1) ensuring cooperation in the area of national defense with the relevant agencies of the North Atlantic Treaty Organization in the area of cybersecurity; 2) coordinating activities in strengthening defense capabilities in the event of a cybersecurity threat; 3) ensuring cooperation between national and allied armed forces in the provision of cybersecurity; 4) developing systems for the exchange of information on cybersecurity threats in the area of national defense; 5) participating in the implementation of the objectives of the North Atlantic Treaty Organization in the area of cybersecurity and cryptology[14]. This provision refers to the basic rules of cooperation and coordination between the Minister of National Defense and the National Contact Point with NATO within the national cybersecurity system in Poland. Also important in this context is free communication between these institutions using specialized and, if necessary, updated national defense cybersecurity threat information sharing systems with their information and communication technologies modules[15].

The organizational units under the authority of the Minister of National Defense include the National Cyberspace Security Center – Cyberspace Defense Forces Component Command (which conducts scientific and educational, research and development, implementation, and advisory activities related to cybersecurity), as well as the Expert Cyber Security Training Center in Warsaw (responsible for shaping the directions of development of the professional training system in the field of cybersecurity, cryptology, and information technology)[16].

Tasks related to cybersecurity are also carried out by the Academic Center for Cybersecurity Policy (ACPC) established by the decision of the Minister of National Defense, including in particular preparation of analyses and expert opinions, reports, and recommendations on cybersecurity, with particular emphasis on legal aspects, for the needs of the National Defense Department, including the managerial staff and other entities operating for the benefit of cybersecurity of the Republic of Poland.

14 Art. 52 of the Act on the National Cybersecurity System imposes on the Minister of National Defense the obligation to maintain the National Contact Point for cooperation with the North Atlantic Treaty Organization, I. Szulc, *Komentarz do art. 52* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.

15 K. Świtała, *Komentarz do art. 52* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

16 Announcement of the Minister of National Defense of January 10, 2022 on the list of organizational units subordinate to the Minister of National Defense or supervised by them (M.P. of 2022, item 32).

The Minister of National Defense is in charge of the Computer Security Incident Response Team operating at the national level (CSIRT MON), which is part of the national cybersecurity system[17]. The purpose of the national cybersecurity system is set out in Art. 4 of the Act on the National Cybersecurity System and is to ensure national cybersecurity, including the uninterrupted provision of key services and digital services, by achieving an adequate level of security of the information systems used to provide these services and ensuring incident handling.

The tasks of the CSIRT MON team, according to Art. 26 sec. 5 of the Act on the National Cybersecurity System, include coordinating the handling of incidents reported by: 1) entities subordinate to the Minister of National Defense or supervised by them, including entities whose information and communication systems or networks are covered by the uniform list of objects, installations, devices and services included in the critical infrastructure[18]; 2) enterprises of special economic and defense importance, in relation to which the Minister of National Defense is the organizing and supervising body for the execution of tasks for national defense[19].

The CSIRT MON team is competent with regard to incidents related to events of a terrorist nature threatening the security of the state defense potential, the Armed Forces of the Republic of Poland, and organizational units subordinate to or supervised by the Minister of Defense. This jurisdiction arises under Article 27 sec. 2 of the Act on the National Cybersecurity

17 See also: K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021, p. 40.

18 The Director of the Government Center for Security shall draw up in cooperation with the relevant ministries responsible for the systems a uniform list of facilities, installations, equipment, and services constituting critical infrastructure divided by systems. The list also distinguishes European critical infrastructure located on the territory of the Republic of Poland and European critical infrastructure located on the territory of other Member States of the European Union that may have a significant impact on the Republic of Poland. The list is classified, Art. 5b section 7 item 1 of the Act of April 26, 2007 on crisis management (consolidated text of the Journal of Laws of 2022, item 261).

19 The list of entrepreneurs of special economic and defensive significance, in relation to which the Minister of National Defense is the organizing and supervising body for the performance of tasks for national defense, is specified in the Regulation of the Council of Ministers of November 3, 2015 on the list of entrepreneurs of special economic & defensive significance (consolidated text of the Journal of Laws of 2020, item 1647). It should be emphasized that the status of an entity of special economic and defensive significance is more of a burden than an opportunity for additional business development, W. Pawłuszko, *Status prawny wybranych przedsiębiorstw kolejowych jako podmiotów o szczególnym znaczeniu gospodarczo-obronnym*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2016, no. 2, p. 113.

System[20]. Tasks related to the recognition, prevention, and detection of events and offenses of a terrorist nature threatening the security of the state defense potential, the Armed Forces of the Republic of Poland, and organizational units subordinated or supervised by the Minister of National Defense are carried out by the Military Counterintelligence Service[21].

A terrorist event is a situation that is suspected to have arisen from a crime of a terrorist nature[22]. A crime of a terrorist nature is an offense, punishable by imprisonment with a maximum of at least 5 years, committed to: 1) seriously intimidate a large number of people; 2) force a public authority of the Republic of Poland or another state or authority of an international organization to take or refrain from taking certain actions; 3) cause serious disturbances in the system or economy of the Republic of Poland, another state or an international organization – as well as to make a threat to commit such an act[23]. Terrorist crimes are intentional, they aim to achieve a specific result of a political nature (weakening the state, changing its policies). The direct victims of an attack are most often treated as a means to that end. This crime does not lose its terrorist nature due to the motives driving the perpetrator if it meets the conditions set out in Art. 115 § 20 of the Criminal Code[24].

The determination of whether or not a given cybercrime is terrorist is made possible by the fulfillment of the elements outlined in the Criminal Code in conjunction with the possibility of its potential classification as a cybercrime[25].

Information and communication technologies have the potential to foster transparency in the operations of public institutions[26]. They also carry

20 See also: M. Nowikowska, *Komentarz do art. 27* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 211.

21 Art. 5 sec. 1 item 2a of the Act of June 9, 2006 on the Military Counterintelligence Service and the Military Intelligence Service (Journal of Laws of 2019, item 687).

22 Art. 2 item 7 of the Act dated June 10, 2016 on counterterrorist operations (consolidated text of the Journal of Laws of 2021, item 2234, as amended).

23 Art. 115 § 20 of the Act of June 6, 1997 – Criminal Code (i.e. Journal of Laws of 2021, item 2345, as amended). See also: A. Michalska-Warias, *Threat to Commit an Offence of a Terrorist Character According to Article 115 § 20 of the Polish Criminal Code – Selected Interpretation Problems*, „Studia Iuridica Lublinensia" 2019, no. 3, p. 41–50.

24 A. Marek, *Komentarz do art. 115* [in:] idem, *Kodeks karny. Komentarz*, Warszawa 2010.

25 M. Smarzewski, *Cyberterroryzm a przestępstwa o charakterze terrorystycznym*, „Ius Novum" 2017, no. 1, p. 69.

26 K. Kaczmarek, *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, no. 1, p. 74.

significant risks, including in the military domain. Accordingly, the Minister of Defense has a special obligation regarding providing security of cyberspace in the military dimension.

Bibliography

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

Chałubińska-Jentkiewicz K., Brzostek A., *Strategie cyberbezpieczeństwa współczesnego świata*, Warszawa 2021.

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.

Dygasiewicz K., Zapadka P., *Zasady korzystania przez banki krajowe z usługi tzw. chmury obliczeniowej społecznościowej w czasach gospodarki COVID lub postCOVID, w świetle Komunikatu Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, no. 1.

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

Kaczmarek K., *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją*, „Cybersecurity and Law" 2021, 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 scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3.

Marek A., *Kodeks karny. Komentarz*, Warszawa 2010.

Michalska-Warias A., *Threat to Commit an Offence of a Terrorist Character According to Article 115 § 20 of the Polish Criminal Code – Selected Interpretation Problems*, „Studia Iuridica Lublinensia" 2019, no. 3.

Nowikowska M., *Komentarz do art. 27* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Pawłuszko W., *Status prawny wybranych przedsiębiorstw kolejowych jako podmiotów o szczególnym znaczeniu gospodarczo-obronnym*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2016, no. 2.

Pelc P., *„Komunikat chmurowy" Komisji Nadzoru Finansowego*, „Cybersecurity and Law" 2020, no. 2.

Pelc P., *The COVID-19 pandemic and the functioning of financial institutions in Poland*, „Cybersecurity and Law" 2020, no. 1.

Pelc P., *Wpływ planowanych przez UE działań i regulacji na instytucje finansowe w Polsce*, „Cybersecurity and Law" 2021, no. 1.

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.

Smarzewski M., *Cyberterroryzm a przestępstwa o charakterze terrorystycznym*, „Ius Novum" 2017, no. 1.

Szulc, *Komentarz do art. 52* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, ed. A. Besiekierska, Warszawa 2019.

Świtała K., *Komentarz do art. 52* [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Czaplicki, A. Gryszczyńska, G. Szpor, Warszawa 2019.

Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008.

Zadania Ministra Obrony Narodowej w zakresie cyberbezpieczeństwa

Streszczenie

Minister Obrony Narodowej jako organ administracji rządowej, którego właściwość rozciąga się również na bezpieczeństwo cyberprzestrzeni w wymiarze militarnym, został wyposażony przez ustawodawcę w określone środki pozwalające na zapewnienie cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej czy w jednostkach mu podległych bądź też przez niego nadzorowanych – w wymiarze militarnym. Minister Obrony Narodowej prowadzi Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, za którego pośrednictwem też realizuje zadania dotyczące bezpieczeństwa systemów informacyjnych.

Słowa kluczowe: cyberbezpieczeństwo, Minister Obrony Narodowej, Siły Zbrojne RP