Tasks of the Minister of National Defence in the Field of Cybersecurity

Krzysztof Wąsowski

Abstract This article is an attempt to analyse the legal position of the Minister of National Defence of the Republic of Poland in the sphere of the national cybersecurity system. The author distinguishes a large number of types of functions of this public administration entity. On the other hand, the author conducts an analysis of cybersecurity competence of the independent bodies responsible for the cyberspace system security in Poland. The author demonstrates that the Minister of National Defence plays a crucial role in the Polish cybersecurity system in the context of the state's external security.

1 The Notion of a Task Within the Domain of Public Administration—The Responsibilities Associated with the Activities of a Public-Administration Authority

The tasks involved in the activities carried out by a public administration authority are described by administrative law commentators as the notion of competence within which a given public administration authority should operate. In this sense, a “task” is often identified with the so-called material competence of a public administration authority.¹ However, the issue of the material responsibility of a public administration authority is worth analysing from a broader perspective. As Z. Cieślak suggests,

(...) the notion of “competence” in this context goes beyond legal categories, because it relates to the fundamentals of creating administrative structures (the organisational structure

¹Cf. Cieślak (2013), p. 81.

K. Wąsowski (✉)

Akademickie Centrum Polityki Cyberbezpieczeństwa/Academic Center for Cybersecurity Policy, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: k.wasowski@akademia.mil.pl

of public administration reflects the structure of its administrative objectives, tasks, and affairs) and the rules of their functioning (...).²

According to the author, “competence” in its broader perspective may be characterised as “the sum, type, and content of affairs encompassed by the legally non-indifferent activities of an entity.”³ On the other hand, from a strictly procedural perspective, competence is interpreted as only a specific “range of matters” assigned by Acts, which a given entity (a public administration authority or judicial authority) should resolve within its statutory powers.⁴ Therefore, legal procedure experts associate the powers and obligations (competence) of a specific authority with the notion of the “legal capacity of authorities”, defining it as a “set of premises exerting a decisive impact on the capacity to take procedural steps in administrative proceedings”, and these premises, in turn, are determined by the norms of procedural law.⁵

Traditionally administrative law commentators generally linked the notion of the “scope of the activities” (competence, or powers and obligations) of a specific authority to the so-called “task norms” regulating the tasks which should be carried out by a specific administrative authority. This approach was linked to the normative system of a specific public administration authority.⁶ Task norms show the subjective correlation between the activities carried out by public administration authorities and the legal forms of conduct attributed to such activities. Therefore, administrative law norms combine a significance for the state political system with the obligations of a substantive law nature. It should also be stressed that when the tasks in the domain of public administration are carried out in specific matters, they are based on “competence norms”.⁷ In the light of the constitutional principle of legality, concerning the activities of public administration authorities (defined in Article 7 of the Constitution of the Republic of Poland⁸), the responsibility of a public administration authority must arise from the provisions of generally applicable law. Structural legal norms regulating competence—whether defined in a broader, political-system-related, or strictly procedural context—should encompass the four basic

²Cieślak (2013), p. 81.

³*Ibidem*; The same author defines “competence” in the context of the administration theory (as opposed to the legal approach) as the “notion describing the static-structural foundations of conduct, the so-called who and what components”. Obviously, this definition is not sufficient within the state-administration system, and must always be accompanied by a description of the functional-dynamic components, because the ability to act (operational capacity) is never equal to the performance (execution). These two actual aspects of conduct, complementing each other, are reflected in the normative approach, and—strictly speaking—in the types of legal norms—see Cieślak (1992), p. 28.

⁴Compare Adamiak (1998), pp. 119–120.

⁵Also, Adamiak (1998), p. 119.

⁶This issue is presented as such by, i.a. Dawidowicz (1974), p. 57 or Filipek (1974), p. 44.

⁷Similarly, Borkowski (1980), also Dawidowicz (1989), p. 18.

⁸Article 7 of the Constitution of the Republic of Poland states “The bodies of public authority shall function on the basis of, and within the limits of, the law.”

components: time, place, subjective features, and the subject of the activities. The essence of the time criterion in the reconstruction of competence (powers and obligations) of the activities of a public administration authority is the basis for the reconstruction of the “rules updating the capacity for action by an individualised entity.”⁹

2 The Position of the Minister of National Defence in the State System

The Minister of National Defence is the central public administration authority, managing the activities carried out by the department of government administration called “national defence”,¹⁰ and a monocratic component of the central collective authority, namely, the Council of Ministers.¹¹ In the light of the Constitution, the Minister of National Defence acts as an intermediary in the authority of the President of the Republic of Poland over the Polish Armed Forces in peacetime.¹² In a hierarchical structure, the role of the Minister of National Defence is threefold. First of all, the Minister of National Defence is an independent authority of the government administration with independent responsibilities and tasks (arising from the Act on the Authority of the Minister of National Defence and the Act on the Tasks of Government Administration¹³). Second, it acts as an entity, being part of a collective authority that is the Council of Ministers subject to the authority of the Prime Minister.¹⁴ Third, the Minister of National Defence is subject to a certain form of command of the President of the Republic of Poland in terms of having power

⁹Similarly, Cieślak (1992), p. 56.

¹⁰See Article 1(1) of the Act of 14 December 1995 on the Authority of the Minister of National Defence, Polish Journal of Laws of 2019, item 196, as amended; (“the AAMND”).

¹¹Cf. Article 1 of the Act of 8 August 1996 on the Council of Ministers, Polish Journal of Laws of 2019, item 1171, as amended; (“the ACM”).

¹²See Article 134(2) of the Constitution of the Republic of Poland, and Article 1(1) of the AAMND—it should also be noted that neither the Constitution of the Republic of Poland nor the AAMND refer to the essence of the role of intermediation of the Minister of National Defence in the command of the President of the Republic of Poland over the Armed Forces of the Republic of Poland in peacetime, or to the forms and courses of the performance of this legal relation. The authorisation to file applications to the President of the Republic of Poland for the conferring of a military rank specified in the Act is the second constitutional duty—attributed strictly to the Minister of National Defence.

¹³The Act on Government Administration Departments (the GAD Act), which uses both the terms “Minister competent for matters of national defence” (Article 19(2) of the GAD Act) and “Minister of National Defence” (Article 19(3) of the GAD Act).

¹⁴See Article 148(2) of the Constitution of the Republic of Poland and Article 6(1) *a contrario* the ACM.

over the Polish Armed Forces in times of peace¹⁵ and conferring the military ranks.¹⁶ On the other hand, as regards the activities of an entity mentioned in the legal norms defining the responsibilities of the Minister of National Defence (apart from the task of “intermediation” in the authority of the President of the Republic of Poland over the Polish Armed Forces in peacetime), its role is limited only to managing the department of government administration called “National Defence”.¹⁷ According to the GAD Act, the National Defence Department (limited in time—which is quite unique in comparison to other departments of government administration—to the “time of peace”) encompasses the following affairs: state defence, the Armed Forces of the Republic of Poland, the security of the cyberspace in the military dimension, the participation of the Republic of Poland in the military projects of international organisations, and fulfilling the military tasks arising from international agreements and offset agreements.¹⁸ The task norm—defining the scope of activities—entrusts to the Minister of National Defence a wide scope of matters, from managing (in peacetime) the entire operations of the Armed Forces through the operational, executive, and personnel matters concerning the performance of state defence tasks, by implementing the commitments arising from the military obligations undertaken by the Council of Ministers, to the performance of tasks as *statio fisci*, a state or local government organisational unit acting for and on behalf of the State Treasury.¹⁹

3 The National Cybersecurity System

Undoubtedly, globally noticeable technological advancements have taken place in the recent decades, especially in the field of telecommunications and information technologies, which have had an increasing (nearly decisive) impact, not only on the economic life of societies, but also on matters of the security of citizens, including national defence and security. Digital technologies provide not only huge opportunities but also pose significant risks, as reflected in the growing number of what is known as computer incidents.²⁰ The situation has been addressed at the supranational level. In particular, in 2013, the European Commission and the High

¹⁵Article 134(2) of the Constitution of the Republic of Poland.

¹⁶Article 134(5) of the Constitution of the Republic of Poland.

¹⁷See Article 1(1) of the AAMND.

¹⁸See Article 19(1) of the GAD Act. The specific statutory proviso, making the attribution of this jurisdiction to the Minister of National Defence conditional on the autonomous responsibilities of the President of the Republic of Poland or other state authorities, forming, at the same time, a rule concerning conflict if any doubts about interpretations arise in the case of so-called overlapping of responsibilities of individual authorities, is worth noting.

¹⁹Cf. Article 2, (1)–(23) of the AAMND.

²⁰The issue has been more extensively discussed in numerous studies and reports, i.e. *The security landscape of the Polish Internet 2016. The annual report on the activities of CERT Polska*, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf. Accessed 11 June 2020.

Representative of the Union for Foreign Affairs and Security Policy published the Communication on a Cybersecurity Strategy of the European Union—An Open, Safe and Secure Cyberspace,²¹ accompanied by a legislative proposal for a Directive concerning cybersecurity. Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union was adopted on 6 July 2016. It imposed on all Member States the obligation to create a system capable of ensuring the necessary level of cybersecurity in information systems in service sectors of key importance for the maintenance of critical societal and/or economic activities, such as energy, transport, banking, financial institutions, health protection, water supply, and digital infrastructure. The specified administrative system, encompassing specialised public administration authorities and related administrative entities (such as Computer Security Incident Response Teams²²), acting in line with the principle of a single point of contact responsible for the cybersecurity, is intended to be the mechanism supporting and coordinating the functioning of the entire system. The NIS Directive obliged the Member States of the European Union to implement its provisions until 9 May 2018 (however, it is an example of so-called minimum harmonisation, not preventing the Member States from extending the level of cybersecurity required under the Directive). While implementing the obligations imposed under the above-mentioned Directive, Poland began legislative action in April 2017 when the Council of Ministers issued Resolution No. 52/2017 adopting a strategic document on cyberspace in the form of the National Framework of Cybersecurity Policy of the Republic of Poland for 2017–2022. At that time, the Ministry of Digital Affairs started work on the draft of the Act implementing the NIS Directive. The process of inter-Ministry agreements and consultations,²³ completed with the decision of the Council of Ministers' handing over the draft of the Act for parliamentary debate, was started on 8 January 2018.²⁴ The bill was submitted to the Sejm on 30 April 2018,²⁵ which adopted the National Cybersecurity System Act.

The main objective of the Act, in force as of 28 August 2018, was to organise and define the functioning of the National Cybersecurity System.²⁶ The statutory objective was reached in the form of a direct regulatory effect encompassing the named

²¹Join (2013) 1 Final, 07.02.2013.

²²CSIRT—Eng. Computer Security Incident Response Teams.

²³The detailed course of the process, and the documentation referring to it, are published on the website of the Government Legislation Centre (Rządowe Centrum Legislacji)—<https://legislacja.rcl.gov.pl/projekt/12304650/katalog/12466714#12466714>. Accessed 11 June 2020.

²⁴See Memorandum of Understanding No. 17/2018 of the meeting of the Council of Ministers held on 26 April 2018 (RM-000-17-18) <https://legislacja.rcl.gov.pl/docs//2/12304650/12466740/12466745/dokument341423.pdf>. Accessed 11 June 2020.

²⁵The Sejm document was given the number 2505. For the detailed course of the Parliamentary work, see <http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505>. Accessed 11 June 2020.

²⁶See the impact assessment of a legal Act concerning the draft of the National Cybersecurity System Act—<https://legislacja.rcl.gov.pl/projekt/12304650/katalog/12466714#12466714>. Accessed 11 June 2020.

sectors of the national economy, defining the criteria for the identification of the operators of essential services, defining the minimum requirements for the information and communications security of the information systems belonging to operators of essential services and digital service providers, and stipulating the statutory requirements and responsibilities of the Computer Security Incident Response Teams in the field of cybersecurity. Undoubtedly, the test concerning the performance of control and supervisory functions of the responsible public administration authorities defined in the law, regardless of whether their status is of a systemic or just functional nature, will be of key importance for the reliable functioning of the system (administrative structure) from the praxeological point of view.

The systematics of the Act was established on the basis of a model entailing a link between a specific state system hierarchy of various categories and functions of public administration authorities and other administrative entities with tasks attributed to them, and correlated with the responsibilities of the administered entities, defined in the law and characteristic for regulatory legal acts. Customarily, the legislators have separated the control powers (slightly excessively combining them with control responsibilities) of the authorised staff of broadly defined administrative entities. The relatively modern penalty system in the form of financial administrative penalties was additionally implemented, and this will undoubtedly strengthen the importance and “effectiveness” of the control procedure. On the other hand, the “penal-administrative” procedure will definitely be the basic instrument for the implementation of the supervisory (*ex-post*) competences, and together with *ex-ante* supervision instruments (especially, involving decisions on permits) should result in a variety of regulating tools allowing the effective stimulation of the conduct of entities functioning on relevant markets.

4 The Task Norms of the Minister of National Defence Within the Framework of the National Cybersecurity System

In the National Cybersecurity System Act, the Minister of National Defence is mentioned in at least four basic state system dimensions. First of all, as the authority competent for these matters and a component of the National Cybersecurity System.²⁷ Second, as an independent coordination-control-management authority having the separate tasks entrusted to it by the legislators.²⁸ Third, as an authority supervising²⁹ the Computer Security Incident Response Team (the CSIRT MON) functioning at the national level. Fourth, as a member of the collegial body (the College for Cybersecurity), being an advisory and opinion-forming authority of the

²⁷See Article 4(17) in conjunction with Article 41(6), (9) and (11) of the NCSA.

²⁸Cf. Chapter 10 of the NCSA.

²⁹This follows directly from Article 2(2) of the NCSA.

Council of Ministers on cybersecurity.³⁰ It should also be noted that the adoption of the law on the National Cybersecurity System modified the Act on the Departments of Government Administration³¹ to some extent, dividing a subdivision component of “cyberspace security”, into a unit functioning within the “civil dimension” (attributing this component to the department of “digitisation”)³² and one functioning in the “military dimension” (attributing this component to the department of “national defence”).³³

As mentioned earlier, the Minister of National Defence is a component of the national security system due to being named in the law as the authority responsible for the cybersecurity of the following sectors: (1) The health-protection sector—encompassing entities subordinate to or supervised by the Minister of National Defence, including entities whose information and communication systems and networks are included in a uniform list of facilities, installations, equipment, and services forming critical infrastructure,³⁴ and encompassing enterprises of special economic and defence importance and their performance of tasks in the field of the national defence, as organised and supervised by the Minister of National Defence;³⁵ (2) The digital infrastructure sector—for entities listed in the same way;³⁶ (3) digital service providers encompassing the same entities as defined above.³⁷

Within the named sectors and in respect of the said digital service providers, due to their status as “authorities competent for cybersecurity”, the legislators entrust to the Minister of National Defence the authority of a superior (“imperial”) nature, encompassing, in particular, (1) the competence to issue decisions on recognising a specific entity as an operator of essential services;³⁸ (2) the competence to issue decisions on the annulment of decisions recognising an entity as an operator of essential services;³⁹ (3) the establishment of a cybersecurity team for a given sector or subsector⁴⁰ (however, in discharging this duty, the authority competent for cybersecurity is obliged to provide information to the operators of essential services in a given sector and to the CSIRT MON, CSIRT NASK, and CSIRT GOV);⁴¹

³⁰See Article 64 in conjunction with Article 66(1)(4)(c) of the NCSA.

³¹See Article 78 of the NCSA.

³²See Article 12a(1) (10) of the GAD Act.

³³See Article 19(1) (1a) of the GAD Act.

³⁴See Article 41(6) in conjunction with Article 26(5) of NCSA in conjunction with Article 5b (7) (1) of the Act on Crisis Management.

³⁵See Article 41(6) in conjunction with Article 26(5) of NCSA in conjunction with Article 5(3) of the Act on Organisation of National Defence Tasks Performed by Entrepreneurs.

³⁶See Article 41(9) in conjunction with Article 26(5) of NCSA.

³⁷See Article 41(11) in conjunction with Article 26(5) of NCSA.

³⁸See Article 5(1) in conjunction with Article 42(1)(2) of NCSA.

³⁹See Article 5(6) in conjunction with Article 42(1)(2) of NCSA.

⁴⁰See Article 44(1) of NCSA.

⁴¹See Article 44(4) of NCSA.

(4) the competence to impose administrative financial penalties⁴² forming instruments of supervision exercised in respect of operators of essential services and digital service providers, and, under exceptional circumstances, also in respect of the head of an operator of an essential service.⁴³ In addition to the clearly defined tasks performed in the capacity of a superior authority, the legislators have entrusted to the Minister of National Defence, being the authority competent for cybersecurity, an entire set of tasks to be carried out in a non-superior, substantive, and technical or organisational capacity, arising from the control and information tasks.⁴⁴

The legislators have entrusted a separate group of tasks to the Minister of National Defence as a specialised, autonomous public administration authority distinguished in the National Cybersecurity System Act.⁴⁵ Within these tasks, the Minister of National Defence was entrusted with various competences, within the scope of the performance of these “superior”,⁴⁶ legal forms of activity, and those of a “non-superior”—control⁴⁷ or strictly organisational⁴⁸ or substantive and technical

⁴²See Article 53(2)(2) in conjunction with Article 74(1) of NCSA.

⁴³See Article 75 of the NCSA.

⁴⁴Examples of such tasks-powers-responsibilities can be found in Article 42(1) of the NCSA, in which the legislators included the possibility of “entrusting certain tasks to be carried out on its behalf (...) to entities subordinate to or supervised by the authority” (Article 42(3) of the NCSA), also including in the form of an “agreement”, (Article 42(4) of the NCSA), in which “the principles for carrying out the supervision over the proper performance of entrusted tasks by the authority responsible for cybersecurity” should be defined (Article 42(5) of the NCSA). To learn more about the issue of the canonical-theoretical concept of an administrative agreement as the legal form of the activities of public-administration authorities, see Cieślak (1982).

⁴⁵See Chapter 10 of the NCSA—“The Tasks of the Minister of National Defence.”

⁴⁶This pertains, *inter alia*, to the superior competence for managing activities concerning incidents in times of a state of emergency (see Article 51(5) of the NCSA) or the operations of the National Contact Point for cooperation with the North Atlantic Treaty Organisation (see Article 52 of the NCSA).

⁴⁷In particular, the procurement of tools for capacity-building for ensuring cybersecurity in the Polish Armed Forces (see Article 51(4) of the NCSA), the assessment of the impact of incidents on the state defence system (see Article 51(6) of the NCSA), the assessment of hazards to cybersecurity in times of a state of emergency (see, *in principio*, Article 51(7) of the NCSA) or the development of the systems for sharing information on cybersecurity in the sphere of national defence (see Article 52(4) of the NCSA).

⁴⁸*Inter alia*, cooperation between the Armed Forces of the Republic of Poland and the appropriate authorities of the North Atlantic Treaty Organisation, the European Union, and international organisations in the field of state defence in terms of cybersecurity (see Article 51(1) of the NCSA); providing the Armed Forces of the Republic of Poland with the capacities to carry out military actions within the national, coalition, and allied systems, when there is a threat to cybersecurity introducing the need to undertake defensive measures (see Article 51(2) of the NCSA); developing the skills of the Armed Forces of the Republic of Poland in ensuring cybersecurity by organising special training projects (see Article 51(3) of the NCSA); and developing tools for capacity-building involving the assurance of cybersecurity in the Armed Forces of the Republic of Poland (see Article 51(4) of the NCSA).

character.⁴⁹ The legislators entrusted the Minister of National Defence with responsibilities involving tasks in the field of cybersecurity in a specific manner.

The legislators have specified the performance of tasks entrusted to the Minister towards the newly established entity, namely, the CSIRT MON, in an extensive and open manner. Apart from the task of “operating” the CSIRT MON (specified in an extensive and open manner), the legislators do not regulate the mutual relations between these two entities, which are critical for the reliability of the cybersecurity system in the sphere of defence. The issue of the status of the CSIRT MON in the state system goes beyond the framework of this study. It may be even said that a specific kind of “discretion” by the Minister in the performance of this task has been sanctioned, to some extent.

On the other hand, the fact that no other powers have been entrusted to the Minister of National Defence as a member of the collegial body, namely, the College for Cybersecurity, recognised as an opinion-forming and advisory authority of the Council of Ministers, is not surprising, because this “gap” results from the essence of the activities of the collegial authority within the framework of which separate responsibilities are attributed only to the chairs of such authorities.⁵⁰

5 Summary

It is hard to resist the impression that the diversity and multiplicity of tasks attributed to the Minister of National Defence within the framework of the National Cybersecurity System can raise many doubts concerning interpretation within the activities of this supreme (constitutional) public administration authority, which can have unpredictable consequences, especially taking into account its undoubtedly highly responsible function within the public-administration system (directly involving state security). In the field of the cybersecurity of the state, special attention should be drawn to building such legal relations that will be an efficient instrument for the prompt making of correct key decisions. They should be characterised by the maximum elimination of any doubts over interpretation, and the avoiding of any overlapping individual tasks and responsibilities. In the field of cybersecurity, the legislators have expressed a precise definition of the tasks entrusted to the Minister of National Defence only in a limited scope, and have allocated to them a specific set

⁴⁹For instance, participation in achieving the objectives of the North Atlantic Treaty Organisation in the fields of cybersecurity and cryptology (see Article 52(5) of the NCSA) or submitting to the competent authorities proposals concerning defensive measures (see *in fine*, Article 51(7) of the NCSA).

⁵⁰The Chair of the National Broadcasting Council who is the Chair of a collegial body, namely, the National Broadcasting Council, and at the same time has separate, independent, and superior responsibilities to issue concession decisions within the framework of the procedures carried out in cooperation (under specific collaborations) with the National Council *in corpore*, is so far the most characteristic example of such “functioning” within the framework of a collegial body.

of legal instruments in the form of appropriate legal actions. Clearly, numerous doubts concerning interpretation can be resolved and eliminated in the course of the authority's practical performance of activities.

References

- Adamiak B (1998) Właściwość organów. In: Adamiak B, Borkowski J (eds) Kodeks postępowania administracyjnego. Komentarz, Warsaw
- Borkowski J (1980) Zakres przedmiotowy kodeksu postępowania administracyjnego w świetle nowelizacji, Państwo i Prawo 5
- Cieślak Z (1982) Porozumienie administracyjne, Warsaw
- Cieślak Z (1992) Zbiory zachowań w administracji państwowej. Zagadnienia podstawowe, Warsaw
- Cieślak Z (2013) Podstawowe instytucje prawa administracyjnego. In: Niewiadomski Z (ed) Prawo administracyjne, Warsaw
- Dawidowicz W (1974) Wstęp do nauk prawno-administracyjnych, Warsaw
- Dawidowicz W (1989) Zarys procesu administracyjnego, Warsaw
- Filipek J (1974) Rola prawa w działalności administracji państwowej, Warsaw-Cracow

Krzysztof Wąsowski PhD, advocate. Graduated from the Faculty of Law and Administration at the University of Warsaw, Poland and ARGO Top Public Management at the IESE Business School in Barcelona, Spain. Adjunct at the Department of Cybersecurity and New Technologies and an expert at the Academic Center for Cybersecurity Policy at the War Studies University in Warsaw. Partner of the law firm “WLP Legal” in Warsaw, Poland.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.