Krzysztof Andrzej Wąsowski*

Cognition of the Minister of National Defense in the scope of cybersecurity

Abstract

The study attempts to analyse the competence and task standards of the Minister of National Defense in the area of the national cybersecurity system. The author distinguishes four types of functions that the Minister of National Defense performs in the created cybersecurity system in Poland. In this system, this entity is at the same time one of the specialized bodies competent for cybersecurity, at the same time the body separate and independent from them, and the entity managing CSIRT MON and a member of the College for cybersecurity.

Key words: Minister of National Defense, jurisdiction, cognition, competence, cybersecurity, threat, nationaldefence, public administration, national system of cybersecurity, digitalinfrastructure

* Dr Krzysztof Andrzej Wąsowski, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: k.wasowski@akademia.mil.pl.

The concept of cognition – jurisdiction of the operation of a public administration body

Cognition is included in the doctrine of administrative law as the jurisdiction within which the administrative body should operate. In this approach, cognition (jurisdiction of the body's operation) is often identified with the competence of a public administration body[1].

It is worth, however, to look a bit wider on the problem of cognition (jurisdiction) of the administrative body. As proposed by Z. Cieślak "(...) the meaning of the term 'jurisdiction' goes beyond legal categories, since it concerns basics of creating administrative structures (organizational structure of the public administration is a reflection of the structure of goals and tasks and administrative matters) and the principles of their functioning (...)"[2]. According to this in the author, in its broad sense, the concept of "jurisdiction" may be characterized as "the sum, type and content of matters falling under legally unindifferent activity of the entity"[3]. On the other hand, strictly procedural jurisdiction means only a specific "scope of cases", with statutory powers that a given entity (public administration body or judicial body) should resolve[4]. Hence, the processualists associate the concept of "legal capacity of organs" with the cognition of the activity of a given authority (its jurisdiction), which they define as a kind of "set of premises determining the ability to take procedural acts in administrative proceedings", and these premises are in turn determined by procedural law norms[5].

In the classic doctrine of administrative law, the concept of "scope of activity" (properties, cognition) of a given body was usually associated with

1 Por. Z. Cieślak, *Podstawowe instytucje prawa administracyjnego* [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2013, s. 81.

2 Ibidem.

3 Ibidem. Ten sam autor definiuje „właściwość" z perspektywy nauki administracji (w odróżnieniu od podejścia prawniczego) jako „pojęcie opisujące statyczno-strukturalne podstawy zachowania, tzn. elementy kto i co. Naturalnie w systemie administracji państwowej określenie to jest niewystarczające i zawsze musi być dopełnione opisem elementów funkcjonalno-dynamicznych, gdyż możność działania (zdolność do działania) nigdy nie jest równoznaczna z jego dokonywaniem (dokonaniem). Te dwa faktyczne, dopełniające się aspekty zachowania znajdują swoje odzwierciedlenie w układzie normatywnym, a ściślej mówiąc – w typach norm prawnych" – zob. Z. Cieślak, *Zbiory zachowań w administracji państwowej. Zagadnienia podstawowe*, Warszawa 1992, s. 28.

4 Por. B. Adamiak, *Właściwość organów* [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 1998, s. 119–120.

5 Ibidem, s. 119.

the so-called task standards, which normalized the sphere of tasks to be carried out by a given administrative entity. This approach was associated with the normative system of a given public administration body[6]. However, only the "postulativeness" of such a position was noticed quite quickly due to the significant relationship between the activities of public administration bodies and the so-called legal forms of action. It even leads to fusion – so unique and characteristic for the branch of administrative law– procedural norms with substantive and legal norms. In such a situation, the basis for implementing the cognition of a given authority in a specific administrative matter will be a competence norm[7].

Pursuant to the constitutional rule of legalism of public authority bodies (clearly exposed in the content of Article 7 of the Constitution of the Republic of Poland[8]), the competence of a public administration body must result from the provisions of generally applicable law. Structurally, legal norms regulating jurisdiction – regardless of whether they are included in a broader, systemic or strictly procedural context – should contain four basic elements: time, place, subjective features and the object of action. The essence of the criterion of time in the reconstruction of the properties (cognition) of the operation of a public administration body is the basis for the reconstruction of "rules that update the possibility of an individualized entity at a given time"[9]. The criterion of place within the norm determining the jurisdiction is usually closely related to the rules relating to territorial divisions (both general and special). The subjective criterion should include the definition of such features of a given administrative entity, such as its legal status, organizational structure, its place in the system of organs, the way it is created, changed or abolished, and finally the whole complex of personal issues related to its functioning[10]. Finally, an extremely important

6 W taki sposób kwestię tę stawia m.in. W. Dawidowicz, *Wstęp do nauk prawno-administracyjnych*, Warszawa 1974, s. 57 lub J. Filipek, *Rola prawa w działalności administracji państwowej*, Warszawa–Kraków 1974, s. 44.

7 Podobnie J. Borkowski, *Zakres przedmiotowy kodeksu postępowania administracyjnego w świetle nowelizacji*, „Państwo i Prawo" 1980, z. 5, także: W. Dawidowicz, *Zarys procesu administracyjnego*, Warszawa 1989, s. 18.

8 Art. 7 Konstytucji RP stanowi: „Organy władzy publicznej działają na podstawie i w granicach prawa".

9 Z. Cieślak, *Zbiory zachowań…*, s. 56.

10 Z. Cieślak zwraca uwagę, że przepisy wyznaczające status prawny podmiotu pełnią w procesie aktualizacji administracji państwowej bardzo ważną funkcję, gdyż nie tylko ogólnie charakteryzują prawnie dany podmiot poprzez swoje usytuowanie na początku sekwencji przepisów rekonstruujących normy prawne, ale również sygnalizują określony

element of the norm specifying the competence (cognition) of a given public administration body is the criterion of the subject of the action, which primarily determines the activation of the entire administrative system or its element (it can be said that it determines the administrative and legal nature of the activity)[11].

The political position of the Minister of National Defense

The Minister of National Defense is a central public administration body managing the department of government administration "national defense"[12], who is also a member of the central collegiate body, which is the Council of Ministers[13]. In the light of constitutional regulations, the Minister of National Defense (listed in the relevant provisions of the Basic Law *in extenso*) performs the function of an intermediary in the exercise of sovereignty over the Polish Armed Forces by the President of the Republic of Poland in peace time[14]. Characteristically for the norms determining the jurisdiction of the Minister of National Defense is the constitution already specified time (peace time). The spatial criterion, in principle, coincides with the territory of the Republic of Poland, however, the specificity of the competence of the Minister of National Defense goes beyond the territorial framework of one state due to the competence norms relating to the extensive international activity of this government administration body. In the hierarchical structure, the Minister of National Defense has a threefold role. Firstly, the Minister of National Defense, an independent government administration body with independent competences and tasks (arising from both the Act on the office of

układ zależności normatywnych w danym systemie organów oraz ogólnie przesądzają o możliwości działania w konkretnej sytuacji" – zob. Z. Cieślak, *Zbiory zachowań…*, s. 58.

11 Por. Z. Cieślak, *Zbiory zachowań…*, s. 61.

12 Zob. art. 1 ust. 1 ustawy z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz.U. z 1996 r. nr 10, poz. 56 ze zm.), dalej: UMON.

13 Por. art. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. nr 106, poz. 492 ze zm.) dalej: URM.

14 Zob. art. 134 ust. 2 Konstytucji RP, a także art. 1 ust. 1 UMON – warto zwrócić przy tym uwagę, że zarówno w treści samej Konstytucji RP, jak i w UMON nie rozstrzygnięto ani o istocie relacji pośrednictwa ministra obrony narodowej przy zwierzchnictwie prezydenta RP nad Siłami Zbrojnymi RP w czasie pokoju, ani o formach i trybach wykonywania tej relacji prawnej. Drugą – ściśle przypisaną ministrowi obrony narodowej – konstytucyjną kompetencją jest wskazane w art. 134 ust. 5 Konstytucji RP upoważnienie do wnioskowania do prezydenta RP o nadanie stopnia wojskowego określonego w ustawie.

the Minister of National Defense and the Act on Government Administration Departments[15]). Secondly, it performs the function of an entity that is part of a collegiate body, which is the Council of Ministers and thus subordinate to the leadership of the Prime Minister[16]. And thirdly, the Minister of National Defense is under the authority of the President of the Republic of Poland in the sphere of exercising authority over the Polish Armed Forces in peacetime[17] and awarding military ranks[18]. On the other hand, in the sphere of the subject of activity described in the norms determining the jurisdiction of the Minister of National Defense (apart from the task of "mediation" in the authority of the President of the Republic of Poland over the Armed Forces of the Republic of Poland in peacetime), it was reduced to performing the function of managing the department of government administration "national defense"[19].

Pursuant to the "departmental" law, the national defense department (temporarily limited – which is a kind of sensation in relation to other government administration departments – to "time of peace") includes matters of: defense of the State, the Armed Forces of the Republic of Poland, cybersecurity in the military dimension, the participation of the Republic of Polish in military undertakings of international organizations and in the field of discharging military obligations arising from international agreements, as well as the issue of offset agreements[20]. The task norm – determining the scope of activity – assigns the Minister of National Defense a wide spectrum of matters – from managing (in peacetime) the overall activity of the Armed Forces through operational, executive and personnel matters in the scope of

15 Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. nr 141, poz. 943 ze zm.), dalej: UDAR, która posługuje się pojęciem zarówno „ministra właściwego do spraw obrony narodowej" (art. 19 ust. 2 UDAR), jak i „ministra obrony narodowej" (art. 19 ust. 3 UDAR).

16 Zob. art. 148 pkt 2 Konstytucji RP, także art. 6 ust. 1 a contrario URM.

17 Art. 134 ust. 2 Konstytucji RP.

18 Art. 134 ust. 5 Konstytucji RP.

19 Zob. art. 19 ust. 1 UDAR. Warto przy tym zwrócić uwagę na swoiste zastrzeżenie ustawowe, uzależniające przypisanie tej kognicji ministrowi obrony narodowej od niezależnych kompetencji prezydenta RP lub innych organów państwowych, co stanowi jednocześnie regułę kolizyjną w przypadku wątpliwości interpretacyjnych mogących zaistnieć w przypadku tzw. skrzyżowania kompetencji poszczególnych organów.

20 Zob. art. 19 ust. 1 UDAR. Warto przy tym zwrócić uwagę na swoiste zastrzeżenie ustawowe, uzależniające przypisanie tej kognicji ministrowi obrony narodowej od niezależnych kompetencji prezydenta RP lub innych organów państwowych, co stanowi jednocześnie regułę kolizyjną w przypadku wątpliwości interpretacyjnych mogących zaistnieć w przypadku tzw. skrzyżowania kompetencji poszczególnych organów.

implementation of the defense tasks of the State, performance of obligations arising from undertaken by the Council of Ministers military commitments to perform tasks as the *statio fisci* of the State Treasury[21]. It is difficult to treat the task standards (also referred to as directional) as the standards defining cognition (jurisdiction) of a given body in the procedural sense (or closely related to it in the case of administrative law, in the substantive sense).These standards determine the content of the public administration, treating it through the prism of the function directly related to the values recognized by the legislator. The result of these norms is a kind of order imposed by the legislator on a given public administration body, that it should strive to implement the values imposed on it through legal norms (expressed in legal regulations)[22].

National Cybersecurity System

There is no doubt that in recent decades there has been a noticeable technological progress, especially in the field of ICT, having an increasing (almost decisive) impact not only on the economic life of societies, but also on the security of citizens, including defense and national security. Digital technologies bring not only huge opportunities, but also significant threats, manifested in the growing number of so-called computer incidents[23]. This situation was met at a supranational level. In particular, the European Commission together with the High Representative of the Union for Foreign Affairs and Security Policy already in 2013 presented a communication on the European Cybersecurity Strategy entitled *Open, secure and protected cyberspace*[24] together with a legislative proposal relating to the Cybersecurity Directive. Directive (EU) 2016/1148 of the European Parliament and of the Council on measures for a high common level of security of network and information systems in the territory of the Union[25] was adopted on July 6, 2016.

21 Por. art. 2 pkt 1–23 UMON.
22 Cieślak Z., *Zbiory zachowań…*, s. 63.
23 Szerzej problematyka ta została ujęta w licznych opracowaniach i raportach, jak m.in. *Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalnościCERT Polska*, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf.
24 Join (2013) 1 Final, 7.02.2013.
25 Dz.Urz. UE L 194 z 19.07.2016, s. 1; dalej: Dyrektywa 2016/1148.

The regulation imposed on all Member States the creation of a system capable of guaranteeing the required level of cybersecurity of the information systems in the service sectors of key importance for maintaining critical socio-economic activities, such as energy, transport, banking, financial institutions, health sector, water supply and digital infrastructure. The instrument intended to support and coordinate the functioning of the entire system is a specific administrative system of specialized public administration bodies and related administrative entities (such as computer incidents response teams[26]) operating on the basis of the single point of contact for cybersecurity issues. Directive 2016/1148 set the European Union Member States time to implement its provisions by May 9, 2018 (except that it is an example of the so-called minimum harmonization, not limiting Member States to extend the level of cybersecurity required by the Directive).

Poland, in fulfilling the obligations imposed on it by the aforementioned directive, began legislative activities in April 2017, when the Council of Ministers adopted resolution No. 52/2017 adopting a strategic document on cyberspace in the form of the National Cybersecurity Policy Framework of the Republic of Poland for 2017–2022. At that time, work began on the draft law implementing Directive 2016/1148 in the Ministry of Digitization. On January 8, 2018, the process of interdepartmental arrangements and consultations was commenced[27], closed with the decision of the Council of Ministers, directing the works on the bill to the Parliament[28]. On April 30, 2018, the bill was submitted to the Sejm[29], which on July 5, 2018 adopted the Act on the national cybersecurity system[30].

The purpose of the Act, which entered into force on August 28, 2018, was primarily to organize and define the functioning of the national cybersecurity system[31]. The implementation of the statutory goal was achieved by covering

26 CSIRT – Computer Security Incident Response Teams.

27 A detailed course of this process together with the documentation can be found at the website of the Government Legislation Center – https://legislacja.rcl.gov.pl/projekt/12304650/ katalog/12466714#12466714.

28 See The Memorandum of Understanding no. 17/2018 of the meeting of the Council of Ministers on April 26, 2018 (RM-000-17-18) – https://legislacja.rcl.gov.pl/docs//2/12304650/12466740/124 66745/dokument341423.pdf.

29 Drukowi sejmowemu nadano nr 2505. Szczegółowy przebieg prac parlamentarnych zob. http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505.

30 Dz.U. z 2018 r., poz. 1560; dalej: UKSC.

31 Zob. Ocena skutków regulacji do projektu ustawy o krajowym systemie cyberbezpieczeństwa – https://legislacja.rcl.gov.pl/projekt/12304650/katalog/12466714#12466714.

the indicated sectors of the national economy with direct regulatory effect, defining criteria for the separation of key service operators, determining the minimum ICT security requirements for information systems of key service operators and digital service providers, as well as establishing statutory cybersecurity requirements and obligations for teams responding to computer security incidents. There is no doubt that from a praxeological point of view for the smooth functioning of the system (administrative system), the test of implementation of the control method and the exercise of supervisory functions by the public administration bodies appointed for this purpose will be crucial, regardless of whether they have acquired such status in the political sense or only functional.

The taxonomy of the Act was built on a model characteristic for regulatory legislation of linking a specific constitutional system of various categories and functions of public administration bodies and other administrative entities with the assignment of tasks correlated with the obligations specified in the Act of administered entities. Traditionally, the legislator has separated control powers (linking them a little over the top with the control powers) to authorized employees of broadly understood administrative entities. A relatively modern sanction system was also introduced in the form of financial administrative penalties, which will undoubtedly increase the weight and "effectiveness" of control proceedings. In turn, the "criminal and administrative" procedure will necessarily become the basic instrument for the implementation of supervisory competences (*ex post*), which, in conjunction with the ex-ante supervision instruments (in particular permitting decisions), should give a wide range of regulatory tools to effectively stimulate behaviour of the entities functioning on the given relevant markets.

Competency standards of the Minister of National Defense under the National Cybersecurity System

As noted by Z. Cieślak, „normy kompetencyjne pełnią z racji swojego umiejscowienia w ciągu norm prawnych rolę czynnika limitującego prawnie ingerencję organów państwowych, regulując podmiotowy i przedmiotowy zakres zastosowania danej formy działania. Odnoszą się zatem bezpośrednio do funkcji działającego podmiotu, wpływają na zakres jego aktywności, a warunkiem ich stosowania jest uprzednia rekonstrukcja norm określających

właściwość i norm regulujących prawne formy działania”[32]. Such a structure, concerning a kind of balance between what is structural and what is functional in administration[33], is essentially to set the subject-subject boundaries of the formal activity of administrative entities, which in turn leads to the conclusion that the competence standards are closely related to legal forms of activity[34]. Thus, the review of competence norms of the Minister of National Defense will be carried out from the point of view of competence norms identified with legal forms of activity.

In the light of the Act on the national cybersecurity system, the Minister of National Defense has been described in at least four basic political systems.

First of all, being an element of the national cybersecurity system, as the competent authority in these matters[35], secondly, as an independent coordination, control and management body in the scope of competences separately assigned to it by the legislator[36], and thirdly, as the authority managing[37] the Computer Security Incident Response Team operating at the national level (CSIRT MON), fourthly as a member of the collegiate body (College) which is the consultative and advisory body of the Council of Ministers in the cybersecurity matters[38].

It should be added that the adoption of the Act on the national cybersecurity system also introduced a change in the Acton government administration departments[39], separating somehow the subdivision of “cyberspace security” into functioning in the “civil dimension” (assigning this element to the section “digitization”)[40] and operating in the “military dimension” (assigning this element to the “national defense” section)[41].

As it has been mentioned above, the Minister of National Defense is an element of the national security system due to the fact that he has been indicated in the act as the authority competent for cybersecurity: 1) for

32 Z. Cieślak, *Zbiory zachowań…*, s. 75.
33 Por. J. Borkowski, *Zagadnienie kompetencji ogólnej i szczegółowej w prawie administracyjnym*, „Studia Prawnicze” 1971, nr 3.
34 Związek ten jest tak ścisły, że jak twierdzi Z. Cieślak, „normy kompetencyjne mają charakter ius cogens” – zob. Z. Cieślak, *Zbiory zachowań…*, s. 75.
35 Zob. art. 4 pkt 17 w zw. z art. 41 pkt 6, 9 oraz 11 UKSC.
36 Por. rozdz. 10 UKSC.
37 Tak wprost stanowi treść art. 2 pkt 2 UKSC.
38 Zob. art. 64 w zw. z art. 66 ust. 1 pkt 4 ppkt c) UKSC.
39 Zob. art. 78 UKSC.
40 Zob. art. 12a ust. 1 pkt 10 UDAR.
41 Zob. 19 ust. 1 pkt 1a UDAR.

the health care sector – including entities subordinate to or supervised by the Minister of National Defence, including entities whose ICT systems or ICT networks are covered by a uniform list of objects, installations, devices and services included in the critical infrastructure[42], as well as including entrepreneurs with special economic and defence significance, in relation to which the Minister of National Defense is the organizing and supervising body for performing the defence tasks[43]; 2) for the digital infrastructure sector – for the entities specified in the same manner[44]; 3) for digital services providers – covering the same entities as specified above[45]. In the indicated sectors and toward the indicated digital services providers, the legislator assigns to the Minister of National Defense, on account of having the status of "the cybersecurity competent authority" authoritative (imperial) competences, which include in particular: 1) competence to issue decisions on the recognition of the entity as a key service operator[46]; 2) competence to issue a decision confirming the expiry of the decision on recognition as a key service operator[47]; 3) establishing a cybersecurity team for a given sector or subsector[48] (with the exception that, as part of exercising this competence, the competent authority for cybersecurity is required to provide information to operators of key services in a given sector and to CSIRT MON, CSIRT NASK and CSIRT GOV)[49]; 4) competence to impose administrative fines[50], which are instruments of supervision exercised against key service operators and digital service providers, and in specific situations also towards the key service operator's manager[51]. In addition to the clearly defined powers of authority of the Minister of National Defense as the authority competent for cybersecurity, the legislator assigned a whole range of competences (presented in the form

42 Zob. art. 41 pkt 6 w zw. z art. 26 ust. 5 UKSC w zw. z art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
43 Zob. art. 41 pkt 6 w zw. z art. 26 ust. 5 UKSC w zw. z art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców.
44 Zob. art. 41 pkt 9 w zw. z art. 26 ust. 5 UKSC.
45 Zob. art. 41 pkt 11 w zw. z art. 26 ust. 5 UKSC.
46 Zob. art. 5 ust. 1 w zw. z art. 42 ust. 1 pkt 2 UKSC.
47 Zob. art. 5 ust. 6 w zw. z art. 42 ust. 1 pkt 2 UKSC.
48 Zob. art. 44 ust. 1 UKSC.
49 Zob. art. 44 ust. 4 UKSC.
50 Zob. art. 53 ust. 2 pkt 2 w zw. z art. 74 ust. 1 UKSC.
51 Zob. art. 75 UKSC.

of "tasks" imposed on this authority) of a non-executive, material-technical or organizational nature resulting from control and information tasks[52].

The legislator assigned a separate group of tasks to the Minister of National Defense as a specialized, autonomous public administration body, separated in the Act on the national cybersecurity system[53]. As part of these tasks, the Minister of National Defense was assigned various competences, both in the scope of implementing "imperious"[54] legal forms of action, and those of a "non-empowering" nature-controlling[55] or *strictly* organizational[56] or material-technical[57].

It is difficult to see *the ratio* of specific separation of the political position of the Minister of National Defense, especially in the context of his location among the authorities responsible for cybersecurity, where the tasks and

52 Przykłady takich zadań-uprawnień-obowiązków znajdziemy choćby w treści art. 42 ust. 1 UKSC, gdzie ustawodawca zawarł możliwość „powierzenia realizowania w jego imieniu niektórych zadań (…) jednostkom podległym lub nadzorowanym przez ten organ" (art. 42 ust. 3 UKSC), w formie „porozumienia" (art. 42 ust. 4 UKSC), w którym winny zostać określone „zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań" (art. 42 ust. 5 UKSC). W kwestiach analizy doktrynalno-teoretycznej koncepcji porozumienia administracyjnego jako prawnej formy działania organów administracji publicznej zob. Z. Cieślak, *Porozumienie administracyjne*, Warszawa 1982.

53 Zob. rozdział 10 UKSC – „Zadania ministra obrony narodowej".

54 Chociażby kompetencja zwierzchnia do kierowania działaniami związanymi z obsługą incydentów w czasie stanu wojennego (zob. art. 51 pkt 5 UKSC), czy też prowadzenie Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego (zob. art. 52 UKSC).

55 W szczególności: pozyskiwanie narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej (zob. art. 51 pkt 4 UKSC), ocenę wpływu incydentów na system obrony państwa (zob. art. 51 pkt 6 UKSC), ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego (zob. art. 51 pkt 7 *in principio* UKSC), czy też rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej (zob. art. 52 pkt 4 UKSC).

56 M.in.: współpraca Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa (zob. art. 51 pkt 1 UKSC), zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych (zob. art. 51 pkt 2 UKSC), rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych (zob. art. 51 pkt 3 UKSC), rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej (zob. art. 51 pkt 4 UKSC).

57 Jak choćby udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii (zob. art. 52 pkt 5 UKSC) lub przedstawianie właściwym organom propozycji dotyczących działań obronnych (zob. art. 51 pkt 7 *in fine* UKSC).

competences of this minister in the military-defense sphere were clearly indicated.

The explanatory memorandum to the draft Act on the national cybersecurity system contains only a brief explanation indicating that "the introduction to the draft Act of a separate chapter on the tasks of the Minister of National Defense aims to take into account its role in the process of supervision over the state's cyber defense, regulating responsibility for the military sphere of the national cybersecurity system and taking into account the functioning of this system during the period of martial law"[58]. It is hard not to get the impression that instead of clarifying possible interpretative doubts, justification of introducing the said separation by the Minister of National Defense formulated in such a way multiplies them even more[59].

A surprising way of creating the competences of the Minister of National Defense is to leave a kind of interpretation gap in the relations of this body with the newly created entity, which is CSIRT MON. In principle, apart from the casual competence assigned to the Minister of National Defense in the regulation defining the "management" of CSIRT MON, the legislator does not regulate the mutual relations of these two entities, which are key to the efficiency of the cybersecurity system in the area of defense. The issues of the political status of the CSIRT MON go beyond the scope of this study.

On the other hand, it is not surprising not to assign any separate powers to the Minister of National Defense as a member of a collegiate body, which is the Cybersecurity College situated as an opinion-making and advisory body of the Council of Ministers, because such "lack" results from the very essence of the collegiate body, within which separate competences are assigned only to chairmen of such bodies[60].

58 Zob. Uzasadnienie do projektu ustawy o krajowym systemie cyberbezpieczeństwa – Sejm RP VIII kadencji, druk nr 2505.

59 Choćby z uwagi na fakt, że nie wszystkie zadania – kompetencje (ba, nawet ich zdecydowana mniejszość) zawarte w art. 51 i 52 UKSC odnoszą się do stanu wojennego. Dodatkowo komplikacje interpretacyjne może powodować przypisywanie specjalnych kompetencji na czas stanu wojennego ministrowi obrony narodowej w sytuacji i tak sporego zamętu kompetencyjnego wprowadzonego postanowieniami Konstytucji RP w zakresie sposobu sprawowania zwierzchności nad Siłami Zbrojnymi RP i szeroko rozumianą polityką obronną państwa między takimi naczelnymi organami administracji państwowej, jak prezydent Rzeczypospolitej Polskiej, Rada Ministrów, prezes Rady Ministrów czy właśnie minister obrony narodowej.

60 Bodaj najbardziej charakterystycznym przykładem takiego „funkcjonowania" w ramach organu kolegialnego jest przewodniczący Krajowej Rady Radiofonii i Telewizji, będący jednocześnie przewodniczącym organu kolegialnego, jakim jest Krajowa Rada Radiofonii

Summary

It is hard to resist the impression that the multitude and diversity of competences assigned to the Minister of National Defense under the national cybersecurity system may in practice lead the operation of this supreme (constitutional) public administration body to various interpretative doubts, which in the undoubtedly highly responsible (directly related to state security) role, which this body performs in the public administration system may have unpredictable consequences.

In the sphere of state security, particular emphasis should be placed on building such legal relations that will be an efficient instrument in quickly making accurate, key decisions. They should be characterized by the maximum elimination of doubts about interpretation and preventing the crossing of individual tasks and competences. In the area of cybersecurity, the legislator only to a small extent specifies the tasks imposed on the Minister of National Defense, assigning them specific legal instruments in the form of appropriate legal forms of operation. Of course, there is still the organ's practice of the body's operation, which is capable to resolve and eliminate many interpretational doubts.

Bibliography

Literature

Adamiak B., *Właściwość organów* [w:] B. Adamiak, J. Borkowski, *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 1998.

Borkowski J., *Zagadnienie kompetencji ogólnej i szczegółowej w prawie administracyjnym*, „Studia Prawnicze" 1971, nr 3.

Borkowski J., *Zakres przedmiotowy kodeksu postępowania administracyjnego w świetle nowelizacji*, „Państwo i Prawo" 1980, z. 5.

Cieślak Z., *Podstawowe instytucje prawa administracyjnego* [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2013.

Cieślak Z., *Porozumienie administracyjne*, Warszawa 1982.

Cieślak Z., *Zbiory zachowań w administracji państwowej. Zagadnienia podstawowe*, Warszawa 1992.

Dawidowicz W., *Wstęp do nauk prawno-administracyjnych*, Warszawa 1974.

Dawidowicz W., *Zarys procesu administracyjnego*, Warszawa 1989.

Filipek J., *Rola prawa w działalności administracji państwowej*, Warszawa–Kraków 1974.

i Telewizji, a jednocześnie posiadający odrębne niezależne władcze kompetencje do wydawania decyzji koncesyjnych w ramach postępowania prowadzonego niejako wspólnie (w swoistym współdziałaniu) z Krajową Radą in corpore.

Legal acts

Ustawa z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz.U. z 1996 r. nr 10, poz. 56 ze zm.).
Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. nr 141, poz. 943 ze zm.).
Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. nr 106, poz. 492 ze zm.).

Kognicja ministra obrony narodowej w zakresie cyberbezpieczeństwa

Streszczenie

Opracowanie podejmuje próbę analizy norm kompetencyjnych i zadaniowych ministra obrony narodowej w zakresie krajowego systemu cyberbezpieczeństwa. Autor wyróżnia cztery rodzaje funkcji, jakie w kreowanym ustroju cyberbezpieczeństwa w Polsce pełni minister obrony narodowej. Podmiot ten jest w tym systemie jednocześnie jednym z wyspecjalizowanych organów właściwych do spraw cyberbezpieczeństwa, a jednocześnie odrębnym i niezależnym od nich organem, prowadzącym CSIRT MON oraz członkiem Kolegium do spraw cyberbezpieczeństwa.

Słowa kluczowe: minister obrony narodowej, właściwość, kognicja, kompetencja, cyberbezpieczeństwo, zagrożenie, obrona narodowa, administracja publiczna, krajowy system cyberbezpieczeństwa, inftrastruktura cyfrowa