The Duties and Legal Status of the Government Plenipotentiary for Cybersecurity and the College for Cybersecurity

Agnieszka Brzostek

Abstract The imposition of the NIS Directive results in the adoption of the NCSA. A special role in this system is played by the Government Plenipotentiary for Cybersecurity, whose primary task is to coordinate activities and implement the government's policy in the field of cybersecurity.

The Plenipotentiary supervises the risk management process of the national cybersecurity system using aggregated data and indicators developed with the participation of competent authorities for cybersecurity matters, CSIRT MON, CSIRT NASK and CSIRT GOV. The Plenipotentiary's tasks in this area also include providing opinions on government documents, including draft legal acts that affect the implementation of cybersecurity tasks.

The Government Plenipotentiary is also one of the members of the College at the Council of Ministers, which acts as an advisory and consultative body on cybersecurity.

The NCSA also indicates the scope of cooperation of the Government Plenipotentiary with the competent authorities for cybersecurity, which concerns cooperation in matters related to cybersecurity with other countries, organisations and international institutions.

1 The Legal Status of the Government Plenipotentiary for Cybersecurity

In the Polish legal system, the term "Government Plenipotentiary" appears in the Act of 8 August 1996 on the Council of Ministers. The Council of Ministers may appoint a Plenipotentiary for specific matters the assignment of which to Members of the

A. Brzostek (✉)

Instytut Prawa/Institute of Law, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland
e-mail: a.brzostek@akademia.mil.pl

Council of Ministers is not advisable.¹ The authorisation of the Government Plenipotentiary to pursue the matters provided for in this article is restricted by Acts relating to the competences of other Ministers.² This general principle constitutes the basis for appointing a Government Plenipotentiary.³

Government Plenipotentiaries are appointed and dismissed by the Prime Minister; the Council of Ministers, by way of an ordinance, specifies the scope of the powers granted to the Plenipotentiary, the manner of supervising his or her activities, and the procedure for providing the Plenipotentiary with substantive, legal, organisational, technical, and administrative support.⁴ The key point is that the Government Plenipotentiary may be either a secretary or an under-secretary of state. The Act on the Council of Ministers mentions the Government Plenipotentiary in the Chapter on Members of the Council of Ministers. At the same time, it does not refer to the Plenipotentiary as a Member of the Council of Ministers. The legal status of the Government Plenipotentiary has been of little to no interest to researchers. This post is treated briefly in the literature, and only in relation to the provisions of the Act on the Council of Ministers.⁵

In the explanatory Statement on the Act on the National Cybersecurity System,⁶ the promoter did not indicate the legal nature of the Plenipotentiary, describing only his or her duties. This does not mean that the Act's promoter treated this issue differently from the way the others did. The indication that the Plenipotentiary is the secretary or under-secretary of state in the Ministry in question places the Plenipotentiary within a specific organisational structure, and at the same time ensures technical and organisational security when fulfilling duties.

Pursuant to Article 37(1) of the Act on the Council of Ministers, the Minister performs his or her duties with the assistance of the secretary and under-secretaries of state, and the Minister's political cabinet. There is no unified position within the jurisprudence or doctrine which defines the status of a secretary of state or an under-secretary of state. It is generally accepted that they serve the role of Deputy Minister. However, the Resolution adopted by the full panel of the Supreme Court indicated

there can be no doubt that the Deputies of the Minister are neither secretaries nor under-secretaries of state who are not Members of the Council of Ministers, and that they cannot be included in government administration authorities. The professional literature describes them as an element in the political (managerial) structure of the Ministry, or, more precisely,

¹Article 10(1) of the Act on the Council of Ministers.

²The Judgment of the Constitutional Tribunal of 9 May 2000, U 6/98, OTK 2000/4/108 (Statement of Grounds 6/98, Judgment of the Constitutional Tribunal 2000/4/108).

³As of 31 October 2019 there were 36 appointed government Government Plenipotentiaries for specific matters; see <https://bip.kprm.gov.pl/kpr/bip-rady-ministrow/organy-pomocnicze/pelnomocnicy-rzadu-i-pr>. Accessed on 10.05.2020

⁴Article 10(3) of the Act of 8 August 1996 on the Council of Ministers, consolidated text, Polish Journal of Laws of 2019, item 1171, as amended.

⁵E.g. Zimmermann (2016), p. 240.

⁶Explanatory statement for the Act on Court Fees in Civil-Law Matters, print 2505. <https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2505> (accessed on 10 May 2020).

as Ministerial assistants, helping to run the Ministry; they are the closest associates of the Minister and the highest officials in the Ministry, but they cannot be assigned the functions of state authorities, because they perform their duties on behalf of, and under the authority of, the Minister.⁷

It should also be noted that the normative body included Article 37 of the Act on the Council of Ministers in Chapter 6 on the “Scope and principles of Ministers’ activities”, which defines the legal position of a Minister as the supreme entity in government administration, managing a specific department of that administration. This gave rise to the Supreme Court’s conclusion that the assistance and cooperation of the secretary and under-secretaries of state are closely related only to those matters which result from managing a designated department of government administration, and thus remain in the sphere of public administration without going beyond its capacity.⁸

In a gloss to the Supreme Court’s Resolution, B. Mik pointed out that the statement which placed the secretary and under-secretary of state in the role of mere assistants and associates of the Minister and top officials of the Ministry was unfounded. One can only concede that

this particular provision, contrary to Article 37(5) of the Act on the Council of Ministers, in comparison with Article 36 of the Act on the Council of Ministers, has been unusually amiss in its wording.⁹

The indication that a literal interpretation is not sufficient to specify what it means for a Minister to perform his or her duties “with the assistance of” the Secretary, Under-Secretary, and the political cabinet, might also raise doubts. B. Mik rightly remarks that the equating of these three functions in one sentence can be misleading, because the purpose of each individual position is different. The Minister’s political cabinet plays an advisory role, and has no means to influence other members of the Ministry. Similarly inappropriate is applying a functional interpretation, classifying all these positions as auxiliary roles. To that extent, the understanding of these functions would be purely service-oriented.¹⁰ In specific regulations, the secretary of state and under-secretary of state may represent the Council of Ministers at the session of the Sejm and Senate,¹¹ and whether they are obliged to resign along with the resignation of the Prime Minister and the Government.¹² Thus, it is unreasonable

⁷The Resolution of the full composition of the Supreme Court of 14 November 2007 BSA (Administrative Court Office) -1410-5/07, pp. 12–13.

⁸The Resolution of the full composition . . . op. cit.-1410-5/07, pp. 25–26 http://www.sn.pl/sprawy/SiteAssets/Lists/Zagadnienia_prawne/EditForm/2007.11.14.Uchwala.pelnego.skladu.SN.pdf, accessed on 14. September 2020.

⁹Mik (2008), p. 166.

¹⁰Mik (2008), p. 166. It is interesting that B. Mik cites an example of the interpretation of Article 115 §13 of the PC when analysing the term public official – an employee of the Government administration who performs a purely service function does not enjoy the status of a public official.

¹¹Article 9(3)(1) of the Act on the Council of Ministers (the Office of the Council of Ministers).

¹²Article 38 of the Act on the Council of Ministers (the Office of the Council of Ministers). More Mik (2008), pp. 166–167.

to reduce these functions to an auxiliary role only. It is appropriate to recognise, as the legislators intended, a secretary of state or an under-secretary of state as the highest-ranking officials in a Ministry, and as a Deputy Minister, insofar as such a replacement has been appointed.¹³

A separate issue is the position of the Government Plenipotentiary within the structure of public administration. The Plenipotentiary acts as a coordinator of cybersecurity activities. The legislators, in Article 4(19) of the NCSA, while detailing a catalogue of entities covered by the national cybersecurity system, did not include the Government Plenipotentiary for Cybersecurity, but cited the position as a separate entity within the structure of the cybersecurity system. The appointment of a secretary of state or under-secretary of state as a Government Plenipotentiary does not imply that the Plenipotentiary is a public-administration authority. This is explicitly stipulated by specific laws,¹⁴ or by the Code of Administrative Procedure.

2 The Duties of the Government Plenipotentiary for Cybersecurity

The duties which the legislators set out for the Plenipotentiary are related to the concepts of the coordination and implementation of the government's policy of ensuring cybersecurity.¹⁵ The term coordination requires explanation here. Coordination is considered to be a legal situation, or a whole group of legal situations, which aims or aim to organise the activities of many entities, or, more precisely, to harmonise these activities.¹⁶ According to the literature, coordination should be understood as the harmonisation of activities undertaken by organisational units of administration in order to achieve the intended goal more easily and in a uniform manner. Coordination involves actions already taken and eliminates discrepancies between them, or it can entail planned actions, and thus prevent their repetition, overlap, or competition between them.¹⁷ It is noted that there are two sides to understanding the concept of coordination. First of all, it is about removing the contradictions which exist or can exist in the present, and this is treated as the negative side of coordination. The positive side consists of identifying and

¹³Mik (2008), pp. 166–167.

¹⁴The legislators defined differently e.g. the responsible bodies of the National Tax Administration—Article 11(1)(2) of the NCSA. indicated explicitly that the Head of the National Tax Administration is the authority responsible for NTA matters. Article (13) (2) indicates that the Head of NTA, who is the Secretary of State in the office supporting the Minister of Finance, is appointed by the Prime Minister at the request of the Minister competent for public finance.

¹⁵Article 60 of the NCSA: the Regulation of the Council of Ministers of 18 March 2018 on the appointment of a Government Plenipotentiary for Cybersecurity, Polish Journal of Laws of 2018, item 587. Act repealed.

¹⁶Góralczyk (2016), pp. 36–40.

¹⁷Zimmermann (2016), p. 230.

recommending such actions which will contribute to better performance by all entities involved in the coordinative situation in the future.¹⁸

Coordination mostly occurs in the decentralised model, but it can also occur in the centralised model of hierarchical subordination, because it consists of unifying and adjusting the activities of entities which might even be organisationally independent of each other. The influence of the coordinator on the behaviour of the coordinated body is indirect, and the coordinator does not assume responsibility from the coordinated body for its actions. As J. Zimmermann points out, the coordination responsibilities are not very formalised, and are fragmentarily defined in the regulations, often with the use of unclear and ambiguous phrases.¹⁹

Cooperation between public-administration authorities is a kind of bond akin to coordination, which can, of course, only occur in a decentralised system. The forms of cooperation are very diverse. Their basic categorisation involves distinguishing the forms resulting from constitutional law and those introduced by substantive law.²⁰ Such cooperation can involve taking concrete actions, as well as drawing up legal acts. The actual process of cooperation can be, for example, the exchange of information and making suggestions. Legal acts specific to this legal and administrative situation should include all bilateral (or multilateral) acts, such as agreements and settlements. They can sometimes constitute the basis for the creation of separate, permanent structures (entities) for the development of cooperation (companies, unions, and associations).²¹

Pursuant to the Regulation of the Council of Ministers of 16 March 2018 on the appointment of the Government Plenipotentiary for Cybersecurity, the secretary of state or the under-secretary of state was appointed the Plenipotentiary in the Ministry of National Defence.²² The explanatory statement to the Act avoided specifying the status of the Plenipotentiary, but it merely announced the appointment to the position.

The duties set out in Article 62 of the Act specify in detail what the coordination activities of the Plenipotentiary should involve. These comprise the following.

- Analysing and assessing the functioning of the national cybersecurity system on the basis of aggregated data and indicators developed with the participation of public-administrative agencies, and agencies competent for cybersecurity—CSIRT (Computer Security Incident Response Team) MON (Ministry of National Defence), CSIRT NASK (Research and Academic Computer Network), and CSIRT GOV.
- Supervising the risk-management process of the national cybersecurity system with the use of aggregated data, and indicators developed with the participation of

¹⁸Góralczyk (2016), pp. 36–40.

¹⁹Zimmermann (2016), pp. 230–231.

²⁰Zimmermann (2016), p. 231 et seq.

²¹Góralczyk (2016), pp. 36–40.

²²§1 (2) of the Regulation of the Council of Ministers on the appointment of a Government Plenipotentiary for Cybersecurity.

authorities competent for cybersecurity—CSIRT MON, CSIRT NASK, and CSIRT GOV.

- Issuing opinions on government documents, including draft legal Acts affecting the implementation of cybersecurity duties.
- Popularising new solutions and initiating cybersecurity activities at the domestic level.
- Initiating national cybersecurity exercises.
- Issuing recommendations regarding the use of IT devices or software at the request of the CSIRT.

This closed catalogue has been supplemented with separate duties which the Plenipotentiary performs in consultation with the respective Ministers. These comprise the following:

- Cooperating with other countries, organisations and international institutions in matters related to cybersecurity
- Undertaking activities aimed at supporting scientific research and the development of cybersecurity technologies
- Undertaking activities aimed at increasing public awareness of threats to cybersecurity and the safe use of the Internet.²³

The Plenipotentiary will also supervise the process of managing the risk of the national cybersecurity system with the use of aggregated data and indicators developed with the participation of authorities competent for cybersecurity—CSIRT MON, CSIRT NASK and CSIRT GOV. His or her responsibilities in this respect will also include issuing opinions on government documents, including draft legal Acts affecting the performance of cybersecurity duties.

In his or her activities, the Plenipotentiary should also popularise new solutions and instigate cybersecurity activities at the national level, initiate national exercises in cybersecurity, and issue recommendations regarding the use of IT devices and software at the request of CSIRT.²⁴ The Plenipotentiary prepares, and submits to the Council of Ministers, by 31 March each year, a report for the previous calendar year containing information on activities in the sphere of ensuring cybersecurity at the national level.

The Act on the national cybersecurity system also indicates the scope of cooperation of the Government Plenipotentiary with the authorities competent for cybersecurity,²⁵ which involves cooperation in matters related to cybersecurity with other

²³Article 62(2) NCSA.

²⁴Article 61(1) NCSA.

²⁵In Article 41 the Act provided the catalogue and scope of responsibilities of the authorised entities. The entities responsible for cybersecurity are (1) for the energy sector—the Minister competent for energy; (2) for the water-transport sector—the Minister competent for the maritime economy and the Minister competent for inland navigation; (3) for the banking sector and the financial market infrastructure—the Polish Financial Supervision Authority; (4) for the health sector, with the exception of certain entities—the Minister competent for health; (5) for the

countries, organisations, and international institutions, undertaking activities aimed at supporting the scientific research and development of cybersecurity technologies, and conducting educational activities aimed at raising public awareness of cybersecurity threats and the safe use of the Internet.²⁶

One of the duties of the Plenipotentiary, as indicated in the Act on the National Cybersecurity System, is cooperation with CSIRT MON, CSIRT NASK, and CSIRT GOV in order to ensure a cohesive and complete risk management system at the domestic level, the implementation of duties to counteract cross-sectoral and cross-border cybersecurity threats, and ensuring coordination to handle reported incidents.²⁷ In accordance with the definition of risk management adopted in the Act, this means the necessity to take coordinated actions related to cybersecurity management with regard to the estimated risk at the domestic level through the cooperation of the above-mentioned entities.²⁸ The Plenipotentiary may decide on the scope of authority of the CSIRTs. Each CSIRT is obliged to account for its scope of authority, as well as take an action to determine the appropriate addressee of the incident report. Where there is disagreement between the CSIRTs on the determination of their scopes of authority in the event of a critical incident, the identification of the CSIRT coordinating the incident handling should be made by the critical incident team. Responsibility for ensuring incident coordination should be acknowledged as the responsibility of the CSIRT which received the report, until possible clarification with the CSIRT expressing doubts about the chosen scope of authority. In a situation where the CSIRT does not clarify these doubts, it is possible to ask the Plenipotentiary for Cybersecurity to indicate the appropriate solution.²⁹

Article 33(8) of the NCSA provides for authorisation for the Plenipotentiary to contact the authority supervising the entity which the recommendation concerned if such an entity does not follow the recommendation. In such a situation the Plenipotentiary informs the person exercising supervision about the failure to follow the recommendation. The supervisory body, within the scope of its powers, may apply supervisory measures. A letter signed by the Plenipotentiary is a sufficient form of contacting the competent authority.³⁰

healthcare sector, including certain entities—the Minister of National Defence; (6) for the drinking water supply and distribution sector—the Minister competent for water management; (7) for the digital infrastructure sector—with the exception of certain entities—the Minister competent for digital affairs; (8) for the Digital infrastructure sector—Minister of National Defence; (9) for digital service providers, with the exception of certain entities, the Minister competent for digital affairs; (10) for digital service providers, including other entities—the Minister of National Defence.

²⁶Article 62(2) NCSA.

²⁷Article 26 NCSA

²⁸Prusak-Górnicka and Silicki (2019a).

²⁹Prusak-Górnicka and Silicki (2019a).

³⁰Prusak-Górnicka and Silicki (2019a).

The Plenipotentiary is one of the entities³¹ which, in accordance with the provisions of the Act, process personal data obtained in connection with incidents and threats to cybersecurity.³²

3 Cooperation Between the Plenipotentiary & the College for Cybersecurity

The Plenipotentiary is also one of the Members of the College of the Council of Ministers who acts as an opinion-giving and advisory body on cybersecurity matters. The scope of responsibility of the College for Cybersecurity is defined in Article 65 of the Act, and covers, in principle, the expressing of opinions on issues related to the policies and plans for counteracting cybersecurity threats; the performance by CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency performing duties under CSIRT GOV, sectoral cybersecurity teams and authorities competent for cybersecurity of duties entrusted to them in accordance with the policies and plans for counteracting cybersecurity threats; the expressing of opinions on cooperation between the authorities managing or supervising CSIRT MON, CSIRT GOV, and CSIRT NASK; cooperation between CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency, and the Minister—a Member of the Council of Ministers responsible for coordinating the activities of secret services, sectoral cybersecurity teams and authorities competent for cybersecurity; the organisation of the exchange of information relevant to cybersecurity and the international position of the Republic of Poland between government administration authorities and on the proposals of the CSIRT MON, CSIRT NASK or CSIRT GOV regarding recommendations on the use of IT devices or software. Apart from the Plenipotentiary, the College comprises the Prime Minister, as the Chair, the Secretary of the College, and the Members of the College.³³

The Act also stipulated that the Prime Minister, in order to coordinate the cybersecurity activities of the government administration, may, on the basis of the College's recommendations, issue binding directives on guaranteeing cybersecurity

³¹These bodies also include the Minister competent for digital affairs, the Director of the Government Centre for Security, and the bodies responsible for digital affairs.

³²Article 39(4) NCSA. For more on this topic—Taczowska-Olszewska (2019), pp. 243–256.

³³Article 66(1) of the Act on the National Cybersecurity System stipulates that the Members of the College are the Minister competent for internal affairs, the Minister competent for digital affairs, the Minister of National Defence, the Minister competent for foreign affairs, the Head of the Chancellery of the Prime Minister, the Head of the National Security Bureau, if appointed by the President of the Republic of Poland, the Minister—a Member of the Council of Ministers responsible for the coordination of the activities of secret services or a person authorised by him or her with the rank of a secretary of state or under-secretary of state, and if the Minister—a Member of the Council of Ministers responsible for coordinating the activities of secret services has not been appointed—the Head of the Internal Security Agency.

at the domestic level and on the operation of the national cybersecurity system, and also request information and opinions in this regard from Members of the Government.³⁴

The Plenipotentiary may, after securing the opinion of the College, issue, change or revoke a recommendation to use IT devices or software, in particular with regard to the impact on public security or an important interest of state security. The entity within the national cybersecurity system may raise objections to the Plenipotentiary regarding recommendations on the use of IT devices or software, if they are having a negative impact on the service provided or the public task implemented, no later than within 7 days from the date of receipt of the recommendation. It is crucial that in the justification for the objection, the entity must indicate and substantiate the negative impact of the recommendation on the service provided or the task implemented. Objections to the recommendation may be made by any of the entities in the national cybersecurity system, i.e. each of the entities listed in Article 4. The Plenipotentiary shall address the doubts immediately, but not later than within 14 days from the date of their receipt, and uphold the recommendations regarding the use of IT devices or software, or issue revised recommendations. The entity in the national cybersecurity system informs the Plenipotentiary, at his or her request, about the manner and scope of taking into account the recommendations regarding the use of IT devices or software. In the event that the recommendation regarding the use of IT devices or software is not being taken into account, this would be the basis for the Plenipotentiary to contact the authority supervising the entity to inform it about their failure to do so.³⁵

IT security testing of the hardware or software used may be performed by each of the three national-level CSIRTs, i.e. CSIRT MON, CSIRT NASK, or CSIRT GOV. It is reasonable to assume that the testing may be started at the CSIRT's own initiative, or at the request of the College for Cybersecurity or the Plenipotentiary for Cybersecurity. The CSIRT is not bound by the submitted testing application, and its initiation remains at the sole discretion of the CSIRT. The purpose of the study is to identify the vulnerabilities which, when taken advantage of, might affect public security or an important interest of state security.³⁶

The Plenipotentiary issues a recommendation after securing the opinion of the College for Cybersecurity on the basis of an application submitted by the appropriate CSIRT regarding the use of IT devices or software. As a consequence, when a vulnerability which may affect public safety, or an important national security interest, is detected, the CSIRT which discovered the vulnerability is obligated to request a recommendation. Therefore, it is unacceptable to issue a recommendation without the College's opinion. The Plenipotentiary also has the power to change or revoke a recommendation, but the change to or revocation of a recommendation also

³⁴Article 67(1) NCSA.

³⁵Article 33(4-8) NCSA. More on the scope of the individual activities of CSIRT Nowikowska (2019), pp. 191–210.

³⁶Prusak-Górnicka and Silicki (2019a).

requires the opinion of the College. The provisions of the Code of Administrative Procedure do not apply to issuing recommendations, and the form in which they are issued is not a form of administrative decision. Therefore, no complaint may be lodged with the administrative court.³⁷ Such recommendations are abstract in nature. In the light of the regulations, it should be assumed that the Plenipotentiary should inform all entities in the national cybersecurity system that can be affected by the vulnerability of issuing the recommendation, using for that action the CSIRT communication channels and the authorities competent for cybersecurity.³⁸

As part of his or her competences, the Plenipotentiary may submit to the Council of Ministers proposals and recommendations regarding actions which should be taken by entities within the national cybersecurity system in order to ensure cybersecurity at the domestic level, and to counteract threats in this regard.³⁹

The Plenipotentiary draws up and submits to the Council of Ministers, by 31 March each year, a report on the previous calendar year containing information on activities which involve ensuring cybersecurity at the domestic level.

The College operates under the Council of Ministers, and its responsibilities are prescribed by law. These comprise the following.

- (1) Policies and plans for counteracting cybersecurity threats.
- (2) The performance by CSIRT MON, CSIRT NASK, and the Head of the Internal Security Agency of duties under CSIRT GOV, the sectoral cybersecurity teams, and the authorities competent for cybersecurity of duties entrusted to them in accordance with the policies and plans for counteracting cybersecurity threats.
- (3) Cooperation between the managing or supervisory bodies of CSIRT MON, CSIRT GOV, and CSIRT NASK.
- (4) Cooperation between CSIRT MON, CSIRT NASK entities, the Head of the Internal Security Agency, and the Minister—a Member of the Council of Ministers responsible for coordinating the activities of special services, sectoral cybersecurity teams, and the authorities competent for cybersecurity.

³⁷Ibidem. The lack of authority to lodge a complaint to the Provincial Administrative Court is limited by Article 3 of the Law on proceedings before administrative courts, as well as by the fact that the recommendation is abstract and does not decide about rights and obligations.

³⁸Prusak-Górnicka and Silicki (2019b).

³⁹Article 63 NCSA. The indicated Regulation of the Council of Ministers also includes the duties of the Government Plenipotentiary for Cybersecurity. These comprise the following. (1) The analysis and assessment of cybersecurity on the basis of aggregated data and the indicators developed with the participation of the government administration authorities and computer security incident response teams operating at the Ministry of National Defence, the Internal Security Agency, and the Scientific and Academic Computer Network—the National Research Institute. (2) Developing new solutions and initiating cybersecurity activities at the domestic level. (3) Issuing opinions on draft legal acts and other government documents affecting the fulfilment of cybersecurity duties. (4) Conducting and coordinating activities carried out by government administration authorities aimed at increasing public awareness of the threats to cybersecurity and the safe use of the Internet. (5) Initiating national cybersecurity exercises. See §2 (2) of the Regulation of the Council of Ministers of 18 March 2018 on the appointment of the Government Plenipotentiary for Cybersecurity.

- (5) The organisation of the exchange of information pertaining to cybersecurity and the international position of the Republic of Poland between government administration agencies.
- (6) Proposals from CSIRT MON, CSIRT NASK, or CSIRT GOV regarding recommendations on the use of IT devices or software.⁴⁰

Along with the Prime Minister as the Chair, and the Plenipotentiary for Cybersecurity, the College comprises the Secretary of the College and the Members. Under the Act the following Ministers are the Members: the Minister competent for domestic affairs, the Minister competent for digital affairs, the Minister of National Defence, and the Minister competent for foreign affairs, as well as the Minister—a Member of the Council of Ministers responsible for coordinating the activities of the secret services or a person authorised by them in the rank of secretary of state or under-secretary of state, and if the Minister—a Member of the Council of Ministers responsible for the coordination of the activities of the secret services—has not been appointed—the Head of the Internal Security Agency. The Members may also include the Head of the Chancellery of the Prime Minister and the Head of the National Security Bureau, if appointed by the President of the Republic of Poland.⁴¹ Depending on the needs and the subject of the sessions, the meetings of the College are also attended by the Director of the Government Centre for Security, the Head of the Internal Security Agency or his or her Deputy, the Head of the Military Counterintelligence Service or his or her Deputy, the Director of the Scientific and Academic Computer Network—the National Research Institute.

The responsibilities of the College include the development of recommendations for the Council of Ministers regarding cybersecurity activities at the domestic level. On the basis of these recommendations, the Prime Minister, in order to coordinate the activities of the government administration, may issue binding guidelines on ensuring cybersecurity at the domestic level, and the operation of the national cybersecurity system, and also request information and opinions in this regard. The Prime Minister issues binding guidelines for CSIRT MON, CSIRT GOV, and CSIRT NASK related to handling critical incidents, including the designation of the CSIRT responsible for handling a specific critical incident.⁴²

4 Summary

Within the scope of his or her activities, a Plenipotentiary coordinates the activities of entities and bodies with authority in cybersecurity. In a closed catalogue, the Act specifies these duties, pointing out their fairly general nature, focusing on the

⁴⁰Article 65(1) NCSA.

⁴¹Article 66(1) NCSA.

⁴²Article 67 NCSA.

assessment of the process of the functioning of the national cybersecurity system, and on issuing recommendations. The legislators did not provide the Plenipotentiary with the responsibilities of a public-administrative authority, thus emphasising its character as a coordinator—not a manager—of cybersecurity activities. It is also related to the legal nature of actions taken by the Plenipotentiary, which do not display the characteristics of an administrative decision, i.e. they exclude the application of the Code of Administrative Procedure. The fact that the Plenipotentiary is not designated as a public-administration authority is also related to the legal status of the Government Plenipotentiary, which, under the Act on the Council of Ministers, becomes a secretary or an under-secretary of state. The College, established as an opinion-giving and advisory body, does not raise any doubts as to its legal status. At present, it is still difficult to assess the activities of both the Plenipotentiary for Cybersecurity and the College. The creation of the cybersecurity system, and the implementation of solutions and recommendations, is ongoing, so it takes time to make a substantive assessment of the activities of the discussed entities, as well as the legal solutions.

References

- Góralczyk W Jr (2016) *Kierownictwo w prawie administracyjnym*, Warsaw
- Mik B (2008) The Gloss to the Resolution Adopted by the Full Composition of the Supreme Court of 14 November 2007, file ref. BSA (Administrative Court Office) – 4110-5/07 (regarding the right of the Minister of Justice to delegate a judge), *Prokuratura i Prawo*, 6
- Nowikowska M (2019) Commentary on Art. 26. In: Kitler W, Taczowska-Olszewska J, Radoniewicz F (eds) *Ustawa o Krajowym Systemie Cyberbezpieczeństwa. Komentarz*, Warsaw
- Prusak-Górnicka K, Silicki K (2019a) Commentary on Article 26 NCSA. In: Czaplicki K, Gryszczyńska A, Szpor G (eds) *Ustawa o Krajowym Systemie cyberbezpieczeństwa. Komentarz*, Warsaw, LEX/el.
- Prusak-Górnicka K, Silicki K (2019b) Commentary on Article 33 NCSA. In: Czaplicki K, Gryszczyńska A, Szpor G (eds) *Ustawa o Krajowym Systemie cyberbezpieczeństwa. Komentarz*, Warsaw, LEX/el.
- Taczowska-Olszewska J (2019) Commentary on Article 39. In: *Komentarz W, Kitler J, Taczowska-Olszewska F (eds) Ustawa o krajowym systemie cyberbezpieczeństwa. Radoniewicz, Warsaw*
- Zimmermann J (2016) *Prawo administracyjne*, Warsaw

Agnieszka Brzostek PhD, adjunct at the Institute of Law of the War Studies Academy. She is a lecturer of law and administrative procedure at studies in the field of law and administration. Scientific interests focus on administrative law and administrative procedure, as well as on the functioning of public administration, in particular on the activities of public administration bodies in the field of security and cybersecurity. Scientific interests focus on administrative law and administrative proceedings, as well as on the operation of public administration, in particular on the operation of public administration bodies in the field of security and cyber security. She is the author or co-author of numerous chapters in monographs and scientific articles.

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.