Agnieszka Brzostek*

The policy of protecting public administration cyberspace based on the example of the government administration authorities indicated in the Act on the National Cybersecurity System

Abstract

The necessity of the implementation of the NIS directive resulted in the adoption of solutions and concepts which would regulate the system of cybersecurity in the cyberspace to the Polish legal order. The directive formulates the obligations to ensure cybersecurity of the information systems in the service sectors which have a key meaning for maintaining critical socio-economic activity and thus energy, transport, banking, financial institutions, the health sector, water supplies and digital infrastructure. The act on the national system of cyber-security, which implements the directive, introduces a new concept to the Polish legal order, and thus a key service operator, digital service provider, and defines the organs responsible for cybersecurity, formulating their scope of tasks and mutual relations.

Key words: national system of cyber security, Government Plenipotentiary for cybersecurity, government administration, digital infrastructure, digital services, threat, security

* Dr Agnieszka Brzostek, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: brzostek.agnieszka@gmail.com.

Preparation of the Act on the national Cybersecurity system[1] was justified by the constantly growing influence of ICTs on the socio-economic development of the European Union Member States. The increase in their use means that the products and services offered are now increasingly dependent on cybersecurity. The developed ICT system, including operations on large data resources, serves the development of communication, trade, transport and constitutes the basis for the functioning of key, digital and public administration services[2]. Therefore, any disruption of this process, whether global or local, will have an impact on the functioning and provision of services, e.g. in the public sector. Bearing in mind the above-mentioned threats, the Ministry of Digitization, as the petitioner of the bill, indicated the necessity of undertaking works on the comprehensive development of the system in the situation of constantly growing and dynamically developing threats in cyberspace. The second impulse was the need to implement into the Polish legal order the Directive of the European Parliament and of the Council (EU) 2016/1148 on the measures for a high common level of security of network and information systems on the territory of the Union (hereinafter the NIS Directive)[3], which was adopted on July 6, 2016. This forced the legislator to create the national system of the government administration authorities and equip the existing ones with new tasks and competences within the scope of implementation of activities in the area of cyber security system. Hence, the need to analyse system solutions and the scope of tasks of government administration authorities indicated in the Act on the national cybersecurity system with the solutions already adopted and implemented in this regard.

Thus, in the beginning the concept of cyberspace needs to be clarified. Limited to the basic conceptual scope only, cyberspace[4] is a space for the processing and exchanging of information created by the communication and information systems defined in Article 3 clause 3 of the Act of February 17,

1 Ustawa z dnia 8 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

2 Uzasadnienie do projektu ustawy o krajowym systemie cyberbezpieczeństwa przygotowane przez Ministerstwo Cyfryzacji, s. 1; dostępne online.

3 Dz.Urz. UE L 194. s. 1.

4 Art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932). Taka sama definicja w art. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928) i w art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558 ze zm.).

2005 on the computerization of the activities of the entities performing public tasks[5], including the links between them and relations with the users. The same definition is repeated in each emergency act. A. Szmyt emphasized that the concept of cyberspace defined in this way is an indeterminate *concept, which appears in the public consciousness as a default concept, with an undetermined normative content, and is a rather colloquial conceptual cluster*[6]; in order to avoid repeating the same definitions, reference should be made to one definition given in one legal act. According to J. Wasilewski, cyberspace is a logically separated area, a digital domain for the processing and exchanging of information. This space, having a transnational character, is created by communication and information systems connected via telecommunications networks, including networks whose infrastructural elements are located in other countries. Cyberspace activity is not limited to the exchange of information only. It may also consist of merely making, modifying or simply reading[7] them. As noted by K. Chałubińska-Jentkiewicz, cyberspace should be treated as a general good enabling the development and undisturbed functioning of the information society. This is due to the fact that cyberspace already covers practically all areas of activity of both human and businesses as well as of the state itself[8].

The need to implement the NIS directive has resulted in the adaptation to the Polish legal system of solutions and concepts that will regulate the cybersecurity system in cyberspace. The directive obliged all EU Member States to guarantee the minimum level of the national cybersecurity capabilities by establishing competent authorities and a single point of cybersecurity,

5 Dz.U. z 2017 r., poz. 1897. Tak skonstruowana definicja została powtórzona także w innych aktach prawnych, np. Polityka ochrony cyberprzestrzeni RP z dnia 25 czerwca 2013 r.

6 A. Szmyt, *Opinia prawna do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (druk sejmowy nr 4355 dostępny online).

7 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 231.

8 K. Chałubińska-Jentkiewicz szerzej opisała zjawisko cyberprzestrzeni w porządku międzynarodowym i krajowym. Szerzej: K. Chałubińska-Jentkiewicz, M. Karpiuk, *Prawo nowych technologii*, Warszawa 2015, s. 61–72. Na ten temat pisała M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeń we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2, s. 19–38, a także J. Skrzypczak, *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7, s. 133–141. Pojęcie cyberprzestrzeni najczęściej występuje w zakresie cyberbezpieczeństwa lub cyberprzestępczości, stąd wiele publikacji dotyczy tych zagadnień.

setting up Computer Security Incident Response Teams (CSIRTs) and adopting national cybersecurity strategies. The directive formulates obligations to ensure cybersecurity of the information systems in key service sectors for maintaining critical socio-economic activity, i.e. in energy, transport, banking, financial institutions, the health sector, water supply and digital infrastructure. It introduces the concept of a key service operator, i.e. an entity providing a key service using information systems, in which ICT security incidents could have a significant impact on its provision[9]. The text of the directive focuses on three pillars: institutions that should be established in all Member States, cooperation at the European level, obligations in the area of network and information security. Within the first pillar, each Member State is obliged to establish competent authorities for network and information security, responsible for monitoring the application of its provisions in sectors falling within its scope. Due to the differences in the national governance structures, Member States may designate more than one national competent authority responsible for performing cybersecurity tasks of key service operators and digital service providers[10]. Furthermore, if many competent authorities have been established, each Member State must establish a Single Focal Point to strengthen cooperation between Member States. The Point will collect information about incidents on a national scale and through contact with its counterparts from abroad will strengthen the exchange of information on significant transnational incidents. The last institution required by the directive is CSIRT, covering the entire subject scope of the regulations[11].

The directive left it up to the national legislator to create a system for the operation of public administration authorities to carry out the tasks specified in the Directive. The Act of July 8 on the national cybersecurity system establishes the competent cybersecurity authorities, the Single Contact Point for cybersecurity, and three teams responding to computer security incidents operating at the national level: 1) led by the Minister of National Defence (CSIRT MON); 2) run by the Scientific and Academic Computer Network – the National Research Institute (CSIRT NASK), and 3) run by the Head of the Internal Security Agency (CSIRT GOV)[12].

9 Pkt 31–33 dyrektywy. Zob. także uzasadnienie do projektu…, s. 3–6.
10 Uzasadnienie do projektu…, s. 6.
11 Ibidem.
12 Ibidem.

To begin with, one should present the national cybersecurity system adopted in Poland, listed in an exhaustive list in article 4 of the aforementioned Act to which belong: 1) key services operators; 2) digital services providers; 3) CSIRT MON; 4) NASK CSIRT; 5) CSIRT GOV; 6) sectoral cybersecurity teams; 7) entities of the public finance sector[13]; 8) research institutes; 9) The National Bank of Poland; 10) Bank Gospodarstwa Krajowego; 11) Technical Inspection Office; 12) Polish Air Navigation Agency; 13) Polish Accreditation Centre; 14) National Fund for Environmental Protection and Water Management and voivodship funds for environmental protection and water management; 15) commercial companies carrying out public service tasks; 16) entities providing cybersecurity services; 17) authorities competent for cybersecurity; 18) Single Contact Point for cybersecurity; 19) Government Plenipotentiary for Cybersecurity; 20) Cybersecurity Board.

The specified directory is a closed directory. The government plenipotentiary for cyber security plays a special role in this system whose main task is to coordinate activities and implement the government's policy in the field of cybersecurity[14]. The plenipotentiary is appointed and dismissed by the Prime Minister. The plenipotentiary is the Secretary of State or Under-Secretary of State. Substantive, organisational, legal, technical, office support for the plenipotentiary is provided by the Ministry or other government administration office in which the plenipotentiary has been appointed. Pursuant to the ordinance of the Council of Ministers of March 16, 2018 on the appointment of a government plenipotentiary for cybersecurity, the Secretary of State or Undersecretary of State in the Ministry of National Defence became the plenipotentiary[15]. The plenipotentiary will coordinate tasks and coordinate government policy by means of analysing and assessing the functioning of the national cybersecurity system based on aggregated data and indicators developed with participation of public administration authorities, authorities competent for cybersecurity, CSIRT MON, CSIRT NASK and CSIRT GOV. The plenipotentiary will also supervise the risk management process of the national cybersecurity system using the aggregated data and indicators developed with

13 Ustawa wskazuje, że są to jednostki, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077 ze zm.).

14 Art. 60 ustawy o krajowym systemie cyberbezpieczeństwa.

15 § 1 ust. 2 rozporządzenia Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 587).

participation of authorities competent for cybersecurity, CSIRT MON, CSIRT NASK and CSIRT GOV.

His tasks in this area will also include giving opinions on government documents, including draft legal acts affecting the implementation of cybersecurity tasks. In his activity, the plenipotentiary should also disseminate new solutions and initiate activities in the area of ensuring cybersecurity at the national level, initiate national cybersecurity exercises and issue recommendations regarding the use of IT devices or software at the request of CSIRT[16]. The plenipotentiary prepares and submits to the Council of Ministers by March 31 each year a report for the previous calendar year containing information on the activities conducted in the area of ensuring cyber security at the national level. Within the scope of its competences, the plenipotentiary may submit to the Council of Ministers proposals and recommendations concerning actions that should be taken by the entities of the national cybersecurity system in order to ensure cybersecurity at the national level and counteract threats in this respect[17].

The Act on the national cybersecurity system also indicates the scope of cooperation of the plenipotentiary with the competent authorities for cybersecurity[18], which concerns cooperation in matters related to

16 Art. 61 ust.1 ustawy o krajowym systemie cyberbezpieczeństwa.

17 Art. 63 ustawy o krajowym systemie cyberbezpieczeństwa. Wskazane rozporządzenie RM także zawiera zadania pełnomocnika rządu do spraw cyberbezpieczeństwa. Należą do nich: 1) analiza i ocena stanu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji rządowej oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego działających w Ministerstwie Obrony Narodowej, Agencji Bezpieczeństwa Wewnętrznego oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym; 2) opracowywanie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym; 3) opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa; 4) prowadzenie i koordynowanie działań prowadzonych przez organy administracji rządowej mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z internetu; 5) inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa. Zob. § 2 ust. 2 rozporządzenia Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa.

18 Ustawa w art. 41 wskazała katalog i zakres kompetencji właściwych organów do spraw cyberbezpieczeństwa, którymi są: 1) dla sektora energii – minister właściwy do spraw energii; 2) dla sektora transportu z transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; 4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 5) dla sektora ochrony zdrowia z wyłączeniem podmiotów – minister właściwy do spraw zdrowia; 6) dla sektora ochrony zdrowia obejmującego podmioty – minister obrony narodowej;

cybersecurity with other countries, international organizations and institutions, taking activities to support scientific research and development of technologies in the area of cybersecurity, and conducts educational activities aimed at raising public awareness of the threats of cybersecurity and secure use of the internet[19].

The plenipotentiary is also one of the members of the Board at the Council of Ministers, which acts as an opinion-forming and advisory authority in the matters of cybersecurity. The scope of competence of the Board for cybersecurity is indicated in article 65 of the Act on Cyber-security and covers, in principle, expression of opinions on issues concerning directions and plans for counteracting cybersecurity threats, performance by CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency, performing tasks within the framework of CSIRT GOV, sectoral cybersecurity teams and authorities competent for cybersecurity tasks entrusted to them in accordance with directions and plans for counteracting cyber-security threats, as well as expressing opinions in the scope of cooperation between the authorities conducting or supervising CSIRT MON, CSIRT GOV and CSIRT NASK, cooperation between the entities of CSIRT MON, CSIRT NASK, the Head of the Internal Security Agency and the minister – a member of the Council of Ministers responsible for coordinating activities of intelligence services, sector cybersecurity teams and authorities competent for cybersecurity; organization of exchange of information essential for cybersecurity and the international position of the Republic of Poland between government administration authorities and on the conclusions of CSIRT MON, CSIRT NASK or CSIRT GOV regarding recommendations on the use of IT equipment or software. The Board, in addition to the plenipotentiary, includes the Prime Minister as the chairman, secretary of the Board and members of the Board[20].

7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej; 8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów – minister właściwy do spraw informatyzacji; 9) dla sektora infrastruktury cyfrowej – minister obrony narodowej; 10) dla dostawców usług cyfrowych z wyłączeniem podmiotów – minister właściwy do spraw informatyzacji; 11) dla dostawców usług cyfrowych obejmujących podmioty – minister obrony narodowej.

19 Art. 62 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa.

20 Ustawa o krajowym systemie cyberbezpieczeństwa w art. 66 ust. 1 wskazuje, że członkami Kolegium są: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, minister obrony narodowej, minister właściwy do spraw zagranicznych, szef Kancelarii Prezesa Rady Ministrów, szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez prezydenta Rzeczypospolitej Polskiej, minister – członek Rady

The Act also specified that, in order to coordinate government administration's activities in the scope of cybersecurity, the Prime Minister may, on the basis of the Board's recommendation, issue binding guidelines on ensuring cybersecurity at the national level and the functioning of the national cybersecurity system, as well as request information and opinions in this regard from members of the government[21].

The Minister of Information Technology plays a key role in the process of implementing the provisions of the Act. Based on Article 45 clause 1 of the Act he is responsible for monitoring the implementation of the Cybersecurity Strategy of the Republic of Poland, recommending areas of cooperation with the private sector to increase cybersecurity of the Republic of Poland; preparing annual reports on major incidents reported by key service operators affecting the continuity of their key services in the Republic of Poland and the continuity of their key services in the Member States of the European Union, and significant incidents reported by digital service providers, including incidents involving two or more Member States of the European Union, as well as gathering information on serious incidents that concern or have been forwarded by another Member State of the European Union. The Minister is also responsible for conducting information activities on good practices, educational programmes, campaigns and training to broaden knowledge and build awareness of cybersecurity, including safe use of the internet by various categories of users, and sharing information and good practices related to reporting serious incidents by operators of key services and incidents important by digital service providers. The Minister also, in compliance with Article 46 clause 1 of the Act has competence in the scope of development and maintenance of the ICT system. He also runs a Single Contact Point[22]. The Minister for Information Technology is also responsible for developing, together with the government plenipotentiary, the ministers responsible for the Cyberspace Security Strategy of the Republic of Poland, which the Council of Ministers adopts by resolutions. The strategy takes into account in particular: 1) cybersecurity goals and priorities; 2) entities involved in the

Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – szef Agencji Bezpieczeństwa Wewnętrznego.

21 Art. 67 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.

22 Art. 48 ustawy o krajowym systemie cyberbezpieczeństwa.

implementation and execution of the strategy; 3) measures to achieve the goals of the strategy; 4) defining measures for readiness, response and restoration of the normal state, including principles for cooperation between the public and private sectors; 5) approach to risk assessment; 6) activities related to cybersecurity educational, informational and training programs; 7) activities related to research and development plans in the area of cybersecurity[23].

The minister in charge of computerisation is obliged to review the provisions of the strategy every two years together with the government's plenipotentiary in charge of cybersecurity.

The Act also distinguishes the tasks of the Minister of National Defence, who is responsible for: cooperation between the Armed Forces of the Republic of Poland and the competent organs of the North Atlantic Treaty Organization, the European Union and international organizations in the area of national defence in the field of cybersecurity, ensuring the capabilities of the Armed Forces of the Republic of Poland in a national, allied and coalition to conduct military operations in the event of a threat to cybersecurity resulting in the need for defence. The Minister is also responsible for developing the skills of the Armed Forces of the Republic of Poland in ensuring cybersecurity by organizing specialized training projects, acquiring and developing tools for building the capacity to ensure cybersecurity in the Armed Forces of the Republic of Poland and assessing the impact of incidents on the state defence system. During martial law, the Minister is responsible for managing incident-related activities and assessing cybersecurity threats, and presenting proposals for defence activities to competent authorities, coordinating – in cooperation with the Minister competent for internal affairs and the Minister competent for computerization – the implementation of tasks of government administration authorities and local government units regarding defence activities in the event of a threat to cybersecurity[24], the Minister of National Defence runs the National Contact Point for cooperation with the North Atlantic Treaty Organizations[25].

The legal solutions presented above have been the subject of numerous consultations and opinions. This fact should be assessed positively, as many aspects that raised reservations were included in the Act. Nevertheless, it is worth looking at these remarks, especially since both government and state

23 Art. 69 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa.
24 Art. 51 ustawy o krajowym systemie cyberbezpieczeństwa.
25 Art. 52 ustawy o krajowym systemie cyberbezpieczeństwa.

administration authorities as well as entrepreneurs and NGOs participated in the consultation process. The Lewiatan Confederation indicated, among others for very broad CSIRT rights in the scope of the possibility to request telecommunications operators to provide information on their activities and the adopted organizational and technical solutions. The introduction of such solutions, in particular bypassing the risk and not taking into account the principle of the adequacy of the security measures used for the identified risks, can significantly reduce the freedom of economic activity and reduce the effectiveness of activities carried out in the field of cybersecurity. Particular attention should be paid to the Confederation's demand on implementing acts, since ordinances have not been subject to consultation, and it is the provisions of implementing acts that will be of significant importance for the entire cyberspace protection system[26]. The National Council of the Judiciary drew attention to the "intersecting subject matter of the draft act" with the applicable Act of April 26, 2007 on crisis management, where the proposed provisions, key services dependent on ICT systems will be subject to the rigors resulting from their inclusion in the uniform list of objects, installations and devices included in the critical infrastructure. For these reasons, the Cybersecurity Act should provide for the mechanisms to control the critical infrastructure protection system resulting from the Crisis Management Act. The Council's doubts were mainly raised by the dualism of regulations regarding the adopted properties of specific ICT systems and services[27]. Therefore, the Minister coordinating special services reported similar comments. Critical infrastructure operators will also be the operators of key services, and this means that they will be forced to report incidents twice.

The minister also expressed concern about the incident reporting system itself, which may be a threat in itself, as it will ultimately contain information on threats that are of key importance to national security[28]. From the point of view of organization and division of competences, the opinion of the

26 Opinia Konfederacji Lewiatan do projektu ustawy o krajowym systemie cyberbezpieczeństwa, online <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=0A099FF-19352F4D9C12582B00030CE28>.

27 Opinia Krajowej Rady Sądownictwa do projektu ustawy o krajowym systemie cyberbezpieczeństwa, online <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?documentId=18D8A80D9E85959AC12582B7004951F6 9>.

28 Opinia ministra koordynatora ds. służb specjalnych do projektu ustawy o krajowym systemie cyberbezpieczeństwa; online<https://legislacja.rcl.gov.pl/docs//2/12304650/12466702/12466705/dokument319798.pdf>.

Minister of National Defence, who issued a negative opinion on the project, was the most interesting. He pointed to the over extensive competences of the Minister for computerisation, at the same time recognizing that it is the Ministry of National Defence that should be the entity that fully exercises military control in the field of cybersecurity[29]. These are just a few remarks received by the Ministry in the process of work on the act. There were so many comments that it is impossible to list all and the entities that participated in the consultations. These remarks were intended to indicate how important and extensive the scope of the regulation is.

The presented scope of tasks and competences of government administration authorities in the scope of cybersecurity does not exhaust the subject in any way. These indications are purely theoretical, as it is too early to assess the practical activity of institutions appointed under the Act and the activities of government administration authorities in the areas of competence that the Act has imposed on them. Implementing these tasks in practice will be of vital importance. First of all, it means creating executive acts that will clarify the operation and mutual relations between public administration authorities and other entities performing tasks in the cyberspace system.

Bibliography

Literature

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeń we współczesnym polskim porządku prawnym*, „Przegląd Prawa Handlowego" 2012, nr 2.

Chałubińska-Jentkiewicz K., Karpiuk M., *Prawo nowych technologii*, Warszawa 2015.

Skrzypczak J., *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9.

Legal acts

Ustawa z dnia 8 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 1560).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (t.j. Dz.U. z 2017 r., poz. 1932). Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz.U. z 2017 r., poz. 1928).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz.U. nr 62, poz. 558 ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz.U. z 2017 r., poz. 2077 ze zm.).

Rozporządzenie Rady Ministrów z dnia 18 marca 2018 r. w sprawie ustanowienia pełnomocnika rządu do spraw cyberbezpieczeństwa (Dz.U. z 2018 r., poz. 587).

29 Opinia ministra obrony narodowej do projektu ustawy o krajowym systemie cyberbezpieczeństwa; online <https://legislacja.rcl.gov.pl/docs//2/12304650/12466702/12466705/dokument319646.pdf>.

Polityka ochrony cyberprzestrzeni administracji publicznej na przykładzie organów administracji rządowej wskazanych w ustawie o krajowym systemie cyberbezpieczeństwa

Streszczenie

Konieczność wdrożenia dyrektywy NIS spowodowała zaadaptowanie do polskiego porządku prawnego rozwiązań i pojęć, które uregulują system cyberbezpieczeństwa w cyberprzestrzeni. dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej. Ustawa o krajowym systemie cyberbezpieczeństwa wdrażająca dyrektywę wprowadza nowe pojęcie do polskiego porządku prawnego, zatem operatora usługi kluczowej, dostawcy usług cyfrowych, a także określa organy właściwe do spraw cyberbezpieczeństwa, formułując ich zakres zadań i wzajemne relacje.

Słowa kluczowe: krajowy system cyberbezpieczeństwa, pełnomocnik rządu do spraw cyberbezpieczeństwa, administracja rządowa, infrastruktura cyfrowa, usługi cyfrowe, zagrożenie, bezpieczeństwo