András Bencsik*
Mirosław Karpiuk**

Cybersecurity in Hungary and Poland. Military aspects

Abstract

Nowadays, ensuring cybersecurity is an important objective of public authority. It must take into account the protection of cybersecurity, both in the current and future perspectives. The state security policy must also take into account its dimension in cyberspace, especially today, where many services are provided through communication and information systems.

A special place in the cybersecurity system is given to cyberspace security in the military dimension. In this regard, both the military administration and civil law entities, both acting for defence, will be competent. Effective military operations are directly linked to new digital technologies. As a result, for the sake of state security (both internal and external), it becomes necessary not only to respond to cyberattacks, but also to counteract them.

Key words: cybersecurity, cyberspace, armed forces, the Minister of National Defence

* Assoc. Prof. András Bencsik, PhD, associate professor of Administrative Law, Faculty of Law, Eötvös Lóránd University, e-mail: bencsik.andras@ajk.elte.hu, ORCID: 0000-0001-5772-9968.

* Prof. Mirosław Karpiuk, PhD, Chair of Administrative Law and Security Studies, Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, e-mail: miroslaw.karpiuk@uwm.edu.pl, ORCID: 0000-0001-7012-8999.

Introduction

In a digital state, communication and information systems become particularly important. They provide not only fast communication, but also aid in the provision of services or the performance of tasks. They are used for a variety of purposes, from entertainment, through communication, education and work, through to digital security. From the perspective of the normal functioning of the state, it is important not only to perform tasks with the use of cyberspace, but also to ensure cybersecurity, including in military terms. The protection of cyberspace must be continuous, not only during crises or conflicts (although especially in these cases) but also when the state is performing its tasks uninterruptedly.

Due to the need to ensure cybersecurity (including that in military terms), knowledge, skills and competencies from the sphere of digital threats, cybersecurity risk management, the protection of information systems and critical infrastructure are required. Professional staff carrying out cybersecurity tasks, with the right knowledge, the right skills, or the right competences, can guarantee the quality of activities protecting cyberspace, contributing to the optimisation of its operation and minimising disruptions occurring in this area.

Particular attention should be paid to the need to increase the resilience of information systems that are used in the military sphere, and as such exposed to cyber threats. Seeking to achieve a level of protection that ensures the uninterrupted operation of information systems must be an important direction of the national defence policy.

In the military sphere, an invaluable role is played by the national cybersecurity system, the purpose of which is to ensure cybersecurity at a national level, including the uninterrupted provision of essential services and digital services, by achieving an adequate level of security of the information systems used to provide these services and ensuring incident handling[1]. Nowadays, cyberspace as an operational domain plays an important role for both offensive and defensive operations, and it must be properly secured, especially against cyber-attacks on critical infrastructure aimed at destabilising the state.

1 Art. 3 of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2020, item, 1369, as amended.), hereinafter: the NCSA.

Military aspects of cybersecurity in Hungary

The public administration (including its organisational structure, its operational mechanisms and its staffing framework) does not (or cannot) remain unchanged, cannot be independent of the trends of the contemporary world, and thus it can be said that public administration is constantly in flux. One of the major challenges of our time is digitalisation in the broadest sense, which has required a reorganisation of both the public administration's approach to citizens and its infrastructure in all the countries of the world.

For the sake of completeness, however, the authors of this paper cannot fail to highlight the undisputed virtues of optimal digitisation of public administration, which are also relevant to our study. The leading foreign literature is unanimous in the view that the use of proven digital tools can have a pull effect, which can legitimise the use of new technological tools in new sectors not previously affected by digitisation. This effect is reinforced by the fact that standardised platforms and other digital solutions from the competitive sector can be easily transferred to public administrations, within certain scope and under certain conditions. In fact, this intermediary, interactive online value creation is a phenomenon also known in the „traditional" offline economy, which generally operates on the technology and infrastructure of a business[2]. On the other hand, it should also be stressed that technological tools can be used to a greater extent to achieve and reinforce the objectives declared as goals to be achieved by national and EU public administration policy (e.g. customer focus, efficiency, subsidiarity, etc.), particularly with regard to the activities of public authorities and the organisation of public services. In this context, we would refer to the indicators of the Digital Economy and Society Index (DESI), which ranks the countries of the Central and Eastern European Union in the bottom third of the scale, particularly in terms of the efficiency of public services[3]. It should also be pointed out, however, that digitisation is not just a matter of the functioning of the state and the development of public services: in addition to civil administration, the use

2 On the competition law aspects of this, see J. Firniksz, *Rangsorolation – a new regulatory issue in the age of platforms and information supply*, https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf [access: 31.07.2022].

3 https://digital-strategy.ec.europa.eu/en/policies/desi [access: 31.07.2022]. According to the index, Hungary ranks 23rd, Slovakia 24th, Poland 25th and the Czech Republic 18th, with slightly better indicators.

of new technologies is also becoming increasingly important in defence administration (including defence and the conduct of military operations). There are legal, IT and military aspects to this, which are worth examining and which could also be used to fine-tune the regulatory environment.

It is also worth pointing out that, however inevitable the emergence of the digital explosion in the public sector may be, experience to date – especially in the CEE region – does not necessarily suggest that it is a complete success story. The reasons for this include the difficulty of taking organisational and procedural aspects into account at the same time, the slow and costly process of building infrastructure, and the general resistance to change (especially in human resources), which is also a classic barrier to innovation[4]. Unfortunately, the military-defence aspect, which is the narrower subject of this study, has, however, extensive experience and international reactions, which show that cyberspace is (has been) more receptive to the application of the technologies indicated than civil administration[5].

The military aspects of cyber defence have become an inescapable priority in the framework of NATO (and Hungary as part of it) defence management. Behind this trend is the realisation that, following the end of the Cold War, cybersecurity activities pose the greatest risk, with cyber warfare emerging as a new phenomenon, with operational effects in cyberspace[6]. The question rightly arises as to what are the specific characteristics of cyber warfare that justify a completely new basis for defining the nature of military operations (and defence). There seems to be a consensus in the authoritative literature that the defining characteristics of cyber warfare are: 1) there are no national borders (this is essentially a consequence of the borderless nature of cyberspace and the diversity of attacks); 2) the warring parties include not only military but also civilian actors (espionage, disruptive or destructive goals are often achieved through the involvement of hacker groups); 3) participants

4 Another unfortunate development is that in Hungary there have recently been several articles which, in addition to presenting the results achieved, emphasise why there is no need or opportunity for further digitisation in public administration. Among others, the study by Erzsébet Fejes and Iván Futó, cited later, can be mentioned in this context.

5 In this context see K. Fekete-Krydis, B. Lázár, *Military Defence*, „Review" 2020, no. 3, p. 44.

6 Cf. T. Tóth, *Introducing the NATO Cyber Defence Centre of Excellence*, „National Security Review" 2018, no. 4, p. 49.

and destinations include international companies, domestic and international service providers and global services[7].

Hungary has been a member of the North Atlantic Treaty Organisation (NATO) since 1999, and therefore Hungary could not have been unaffected by the trends and reactions that have emerged in recent years in relation to cyber warfare within NATO. NATO was confronted with cyber warfare for the first time this year, following the bombing of Kosovo, and the cyberattacks detected were carried out initially by the Serbian hacker group Black Hand, and then by Chinese and Russian hackers following the bombing of the Chinese Embassy. The story had both indirect and direct international consequences. The following developments are worth highlighting: 1) following the 2002 NATO summit in Prague, the development of a NATO cyber defence policy came to the fore[8]; 2) at the 2014 Wales Summit, NATO's cyber defence policy guidelines were adopted and cyber defence was included in the collective defence tasks[9]; 3) in 2016, in the final document of the Warsaw Summit, the Allies extended the scope of operational warfare to cyberspace and declared that a cyberattack against a NATO member state could be considered an attack against the Alliance as a whole and could be subject to collective response if necessary[10]; 4) at the 2018 Brussels Summit, it was declared that, while NATO is focused on developing collective defence cyber capabilities, member states are building a full range of capabilities for deterrence and effective action[11].

For reasons of scope, this study cannot provide an overview of NATO's cyber defence activities, so we will now focus on the legislative developments made by the Hungarian legislator to achieve the Alliance's objectives. Among the Hungarian legislative developments, the present study will focus on a relatively new piece of legislation catalysed by NATO's cyber defence policy,

7 See *Cyber warfare and military cyber defence*, https://11686cc6-54a5-8388-87db-54233ab8a32d [access: 22.11.2022].

8 For more on this, see A. Tóth, *Resolutions and agreements following the Prague NATO Summit on the modernisation of the command and control system and the development of joint operational capability*, „Hadmérnök" 2016, no. 3, p. 214.

9 Wales Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, https://www.nato.int/cps/en/natohq/official_texts_112964.htm [access: 23.11.2022.]

10 Warsaw Summit Communiqué issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm [access: 23.11.2022].

11 Brussels Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm [access: 23.11.2022].

namely Act L of 2013 on the Electronic Information Security of State and Local Government Bodies.

The rationale behind the adoption of the legislation is essentially based on the recognition that Hungary, like many other countries in the world, considers cybersecurity a national security issue of high priority[12]. The legislation is both new and old: while it can be noted that information security regulation in Hungary dates back 30 years, the legislative product under consideration can be considered novel in several respects. In this respect, the novae can be identified below: 1) no legislation had previously regulated the IT security of public administrations; 2) since then, there has been a separate regulation on critical infrastructure protection, with which the protection of critical information infrastructure fits in; 3) there have been bodies in the past that have (also) dealt with cyber defence, without a legal basis, in the absence of regulation[13].

The legislation has been the subject of serious professional-political debates in the literature and (in the legislative debate) among certain opposition parties, even before it is actually applicable. One of the most serious concerns is the scope of the law, since at the time of its adoption there was no inventory of critical information infrastructures, which meant that the legislator was forced to designate these actors, in terms of legal security[14].

The other key issue of the reservations is the so-called „Big Brother" effect, the real risk of which is not yet supported by a legal context: on the one hand, it should be stressed that the authorities have had legal means to monitor the electronic activities of certain citizens, and on the other hand, according to some representatives of the literature[15], it is precisely a properly functioning information security system that can provide a control that can strengthen the transparency of organisations.

From the discussion presented in this short paper, it is clear that the Act will result in a forced redesign in the state and local government sector, with the legislator's not hidden aim of providing a predictable path for the organisations

12 Cf. C. Krasznay, L. Muha, *Cyber defence in Hungary: a blessing or a curse?*, „HWSW Online IT News Magazine" 2013, no. 3.

13 Here we mention the National Security Service, of which the National Cyber Defence Institute is now part.

14 This obligation was fulfilled by the legislator with the creation of Government Decree No. 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 on the identification, designation and protection of critical systems and installations.

15 In this context see C. Krasznay, L. Muha, op. cit.

concerned, on the one hand, and (in justified cases) the possibility of immediate intervention, on the other hand, if the inadequate operation of an organisation in cyberspace is objectionable for reasons of national security.

Military aspects of cybersecurity in Poland

The development of new technologies, including military ones, contributes to a significant increase in the employment of unmanned and autonomous systems, automated and robotised weapon platforms using artificial intelligence, as well as long-range precision weapon systems, including ballistic and cruise missiles. Digital technologies are advancing dynamically, which creates the necessity for their efficient use. The development of solutions based on fixed and mobile broadband networks, and artificial intelligence, creates new development opportunities, whilst unfortunately creating previously unknown threats. The challenge for the state is to join the technological race in this area[16]. Conducting military operations (of a defensive nature) in cyberspace is a fundamental task of the state, including military administration. These measures must be adequate to the degree of the threat, must keep up with the dynamics of the development of new technologies used in this sphere, including the use of modern solutions applicable in the world, in order not only to effectively combat cyber threats, but also to prevent them. Civilian actions taken in cyberspace also need to correspond to the dynamics of the development of new technologies in cyberspace, as this also translates into the efficiency of the state and its institutions in carrying out public tasks.

Cybersecurity, as defined in Art. 2(4) of the NCSA, is the resilience of information systems against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[17]. In the case of military cybersecurity,

16 *National Security Strategy of the Republic of Poland*, Warszawa 2020, p. 7–8. See also M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1, s. 49.

17 For more information about cybersecurity refer to: W. Pizło, *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, ibidem 2021, no. 2; K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, *The legal status of public entities in the field of cybersecurity in Poland*, Maribor 2021; M. Karpiuk, *Activities of local government units in the scope of telecommunication*,

information systems will be used by military entities, and civilian ones to the extent in which they work for defence.

Ensuring cybersecurity is one of the basic tasks of public authorities, especially due to the fact that threats of an IT nature are increasingly dangerous and cyberattacks can be used as a means of political pressure[18]. The implementation of this task can take place in the military sphere, and it may involve the use of military telecommunications systems.

One of the authorities competent for cybersecurity in the military sphere is the Minister of National Defence. The Minister of National Defence manages the national defence department which, during peacetime, handles the following issues: 1) the defence of the state and the Armed Forces of the Republic of Poland; 2) cyberspace security in the military dimension; 3) the participation of the Republic of Poland in the military undertakings of international organisations and in the discharge of military obligations under international agreements; 4) offset agreements[19]. In the military sphere, the Minister of National Defence is the executive body in matters relating to ensuring cybersecurity. He performs tasks in this regard through subordinate and supervised organisational units.

The Armed Forces of the Republic of Poland, being a core element of the state's defence system, should engage in cyberspace operations at the same level as they do in their in air, land and sea operations, in peacetime, war and in crisis situations. Cyberspace activities undertaken by the military must include

„Cybersecurity and Law" 2019, no. 1; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; I. Hoffman, K.B. Cseh, *E-administration, cybersecurity and municipalities – the challenges of cybersecurity issues for the municipalities in Hungary*, „Cybersecurity and Law" 2020, no. 2; M. Karpiuk, *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; I. Hoffman, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem 2022, no. 1; M. Czuryk. *Special rules of remuneration for individuals performing cybersecurity tasks*, ibidem, no. 2.

18 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, ibidem 2019, no. 1, p. 145.

19 Art. 19 of the Act of 4 September 1997 on Government Administration Departments (consolidated text, Journal of Laws 2021, item 1893, as amended). See also M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1, p. 86–87.

identifying threats, protecting and defending ICT networks and systems, and combating sources of cyber threats[20].

Cyberspace security in the Armed Forces of the Republic of Poland is to be provided by the Cyberspace Defence Forces. They are a specialist component of the Armed Forces of the Republic of Poland and form a part thereof. They are tasked with performing the full spectrum of activities in cyberspace. In particular, this includes proactive protection and the active defence of elements and the resources of cyberspace relevant to the Armed Forces of the Republic of Poland[21].

Cyberspace Defence Forces are part of the Armed Forces of the Republic of Poland, but they are not a type of, but a component of, them. It should be mentioned here that the supreme Commander of the Armed Forces of the Republic of Poland is the President of the Republic of Poland. In peacetime he has command over the Armed Forces of the Republic of Poland through the Minister of National Defence[22].

Cyberspace (in which the Cyberspace Defence Forces operate) is construed as the space for processing and exchanging information created by communication and information systems, including relations between them and relationships with users[23]. In turn, a communication and information system is a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type[24].

Pursuant to Art. 23(1) of the AHD, the Defence Force Cyberspace Component Commander is competent to command military units and

20 Cybersecurity Strategy of the Republic of Poland – Annex to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Official Gazette of the Republic of Poland 2019, item 1037).

21 Art. 15(4) of the Act of 11 March 2022 on Homeland Defence (Journal of Laws 2022, item 655, as amended), hereinafter: the AHD.

22 Art. 134(1–2) of the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws of 1997, no. 78, item 483, as amended), hereinafter: the Polish Constitution. See also M. Karpiuk, *Prezydent Rzeczypospolitej Polskiej jako organ stojący na straży bezpieczeństwa państwa*, „Zeszyty Naukowe AON" 2009, no. 3, p. 392.

23 See Art. 2(1b) of the Act of 29 August 2002 on Martial Law and the Competences of the Commander-in-Chief of the Army and the Rules of Commander-in-Chief's Subordination to the Constitutional Authorities of the Republic of Poland (consolidated text, Journal of Laws 2017, item 1932, as amended), hereinafter: the AML

24 Art. 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (consolidated text, Journal of Laws 2021, item 2070, as amended).

organised forces of the Cyberspace Defence Forces and is subordinate to: 1) the Minister of National Defence until the appointment of the Commander-in-Chief of the Armed Forces; 2) the Commander-in-Chief of the Armed Forces upon their appointment and their assumption of the command of the Armed Forces. A military unit is defined in Art. 2(12) of the AHD as an organisational unit of the Armed Forces of the Republic of Poland that operates on the basis of an established document issued by the Minister of National Defence and uses an official seal with the emblem of the Republic of Poland and the name (number) of the unit. In turn, an organised force, pursuant to Art. 2(38) of the AHD, means military units organised by the Minister of National Defence into a specific structure, in particular into a corps, division or brigade, operating independently or as part of a type of the Armed Forces of the Republic of Poland, on the basis of the establishment documents issued.

The subordination of the Armed Force Component Commander is explicitly stated in Art. 23(1) of the AHD. He is subordinated to the Commander-in-Chief of the Armed Forces. However, this function is not continuous. The President of the Republic of Poland, in coordination with the President of the Council of Ministers (upon his request), appoints him for the duration of the war. Consequently, he will function in the military structure of the state in the event of a special (qualified) security threat. In the event that the Commander-in-Chief of the Armed Forces has not been appointed, the Defence Force Cyberspace Component Commander is subordinated to the Minister of National Defence.

For the duration of war (the duration of warfare on the territory of the Republic of Poland), the President of the Republic of Poland appoints the Commander-in-Chief of the Armed Forces, as required under Art. 134(4) of the Constitution of the Republic of Poland[25]. From the perspective of the subordination of the Commander of the Cyberspace Defence Forces to the Commander-in-Chief of the Armed Forces, a mere appointment is not enough, as the latter must take command of the Armed Forces of the Republic of Poland.

As stipulated in Art. 23(2) of the AHD, the duties of the Defence Force Cyberspace Component Commander include in particular: 1) implementing the development programme of the Armed Forces of the Republic of Poland;

25 See also M. Kołodziejczak, *Funkcjonowanie Naczelnego Dowódcy Sił Zbrojnych w Rzeczypospolitej Polskiej*, Warszawa 2020, p. 65.

2) programming, planning, organising, conducting and supervising the training courses falling within the jurisdiction of the Defence Force Cyberspace Component Commander that are provided to the subordinate military units and organised forces, organisational cells and units, as well as institutions, bodies and entities, on the basis of concluded agreements; 3) planning and organising the development in the area of mobilisation and operation and the use of Cyber Defence Forces; 4) building, maintaining and protecting infrastructure, as well as protecting information in cyberspace; 5) conducting activities and operations in cyberspace; 6) providing support for military operations conducted by the Armed Forces of the Republic of Poland and operations in the allied and coalition system; 7) working in tandem with other bodies and entities in matters related to state defence; 8) managing and conducting inspections of subordinate military units and organised forces. The Defence Force Cyberspace Component Commander performs his tasks with the assistance of the Defence Force Cyberspace Component Command.

It should be pointed out that there is the need to develop the capabilities of the Armed Forces of the Republic of Poland to conduct operations in cyberspace. Due to the status of this formation, it is the Armed Forces that have the greatest obligation to provide cybersecurity in the military dimension. Hence, in order to meet this obligation, they must have adequate financial and legal resources, as well as adequate personnel.

Cybersecurity can also become a rationale for imposing martial law. According to Art. 2(1–1a) of the AML, in the event of an external threat to the state, including one caused by acts of a terrorist nature or acts in cyberspace, the President of the Republic of Poland may, at the request of the Council of Ministers, impose martial law on part or all of the state's territory. An external threat to the state is construed here as intentional actions which are detrimental to the independence and indivisibility of the territory, important economic interests of the Republic of Poland, or which aim to prevent or seriously disrupt the normal operation of the state, undertaken by entities that are external in relation to it.

Bibliography

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

Cyber warfare and military cyber defence, https://11686cc6-54a5-8388-87db-54233ab8a32d [access: 22.11.2022].

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3.

Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2.

Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.

Fekete-Krydis K., Lázár B., *Military Defence*, „Review" 2020, no. 3.

Firniksz J., *Rangsorolation – a new regulatory issue in the age of platforms and information supply*, https://kti.krtk.hu/wp-content/uploads/2022/01/vesz2021_6-FirnikszJ.pdf [access: 31.07.2022].

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

Hoffman I., Karpiuk M., *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, „Cybersecurity and Law" 2022, no. 1.

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

Karpiuk M., *Activities of local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.

Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.

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

Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

Karpiuk M., *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2.

Karpiuk M., *The Protection of State Security in Cyberspace as a Justifying Ground for Restricting Constitutional Freedoms and Rights*, „Przegląd Prawa Konstytucyjnego" 2022, no. 3.

Kołodziejczak M., *Funkcjonowanie Naczelnego Dowódcy Sił Zbrojnych w Rzeczypospolitej Polskiej*, Warszawa 2020.

Krasznay C., Muha L., *Cyber defence in Hungary: a blessing or a curse?*, „HWSW Online IT News Magazine" 2013, no. 3.

Pizło W., *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Tóth A., *Resolutions and agreements following the Prague NATO Summit on the modernisation of the command and control system and the development of joint operational capability*, „Hadmérnök" 2016, no. 3.

Tóth T., *Introducing the NATO Cyber Defence Centre of Excellence*, „National Security Review" 2018, no. 4.

Cyberbezpieczeństwo na Węgrzech i w Polsce. Aspekty militarne

Streszczenie

Zapewnienie cyberbezpieczeństwa stanowi obecnie ważny cel działania władzy publicznej. Musi ona ochronę cyberbezpieczeństwa uwzględniać w polityce zarówno bieżącej, jak i przyszłej. Polityka bezpieczeństwa państwa musi uwzględniać także cyberprzestrzeń, zwłaszcza obecnie, ponieważ wiele usług jest świadczonych za pośrednictwem systemów teleinformatycznych.

Szczególne miejsce w systemie cyberbezpieczeństwa zajmuje bezpieczeństwo cyberprzestrzeni w wymiarze militarnym. W tym zakresie będzie właściwa zarówno administracja wojskowa, jak i podmioty cywilne, ale działające na rzecz obronności. Skuteczne działania militarne są bezpośrednio związane z nowymi technologiami cyfrowymi. W związku z powyższym ze względu na bezpieczeństwo państwa (zarówno wewnętrzne, jak i zewnętrzne) konieczne staje się nie tylko reagowanie na cyberataki, lecz także im przeciwdziałanie.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, siły zbrojne, Minister Obrony Narodowej