András Bencsik*
Mirosław Karpiuk**

# The legal status of the cyberarmy in Hungary and Poland. An overview[1]

**Abstract**

Cybersecurity tasks concern not only civilians but also the military. Similar to other spheres, cyberspace, as an operational domain, is exposed to threats. This includes destructive threats, ones that destabilise the state or its institutions. Given the need to ensure cybersecurity in the military dimension, individual states establish cyber armies to safeguard the stability of cyberspace, which is exposed to constant attacks. Cyberspace defence in a digital state, where ICT systems are also used to complete military tasks, must be considered a priority not only in national but also in international defence policies.

Key words: cyberarmy, cyberspace, cybersecurity

* Assoc. Prof. András Bencsik, PhD, 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.

**1** Th is article is based upon work from COST Action CA20123 – Intergovernmental Coordination from Local to European Governance (IGCOORD), supported by COST (European Cooperation in Science and Technology). Project no. TKP2021-NVA-29 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

## Introduction

The systemic position of the Armed Forces of the Republic of Poland is defined by the Constitution of the Republic of Poland[2], and more specifically by Article 26, under which the Armed Forces of the Republic of Poland shall safeguard the independence and territorial integrity of the State, and shall ensure the security and inviolability of its borders. At the same time, they shall maintain neutrality in political matters and be subject to civilian and democratic control.

The objectives set for the armed forces (in both Poland and Hungary) also apply to cyberspace, since ICT systems are now also used to perform military tasks.

At a time when ICT systems form the basis for many areas of public, private or social activities or serve as instruments that significantly facilitate such activities, they must not only develop dynamically but also be suitably protected[3]. To ensure the proper functioning of the state and the performance of tasks using cyberspace, it will be necessary to provide cybersecurity, including in the military dimension. The protection of cyberspace must be continuous, not only during crises or conflicts (though in such cases it is particularly important), but also when the state carries out its tasks in an undisturbed manner (preventively)[4].

In the military sphere, emphasis should also be placed on cybersecurity. The Polish legislator defines this as the resilience of information systems against actions that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by said systems[5].

**2** Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).

**3** M. Karpiuk, *The executive agency as a legal organisational form of implementing cybersecurity tasks*, „Cybersecurity and Law" 2023, no. 1, p. 50.

**4** A. Bencsik, M. Karpiuk, *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1, p. 83.

**5** Art. 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws of 2023, item 913). Regarding cybersecurity, see also: K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1; M. Karpiuk, *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2; M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; M. Karpiuk, *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2; P. Krawczyk, J. Wiśnicki, *Information warfare tools and techniques in the context of information operations*

The organisation of the state (including its organisational structure, its operating mechanisms and its personnel framework) does not (cannot) remain unchanged, cannot be independent of the trends of the world of our time, and is therefore in a state of constant flux. One of the greatest challenges of our time is digitalisation in the broadest sense, which has required a reorganisation of the public administration's approach to citizens, of its infrastructure and of the types of public activity of a defensive nature in all the States of the world.

A novel aspect of digitalisation in a broader sense is cybersecurity (which can be understood as, among other things, information security and infrastructure, and closely related to this, the active and passive side of cyber defence (which is more in terms of state violence organisations performing defence functions). This topic cannot be considered a completely new field of law, as it has indirect and direct antecedents in the history of war), but the

*conducted by the Russian Federation during the 2022 war in Ukraine*, ibidem 2022, no. 2; M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3; M. Karpiuk, *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1; M. Nowikowska, *The right to privacy in cyberspace* [in:] *Human Rights as a Guarantee of Smart, Sustainable and Inclusive Growth*, eds. I. Florek, I. Laki, Budapest 2022; M. Karpiuk, *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, no. 2; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Rocznik Nauk Społecznych" 2023, no. 2; M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2; A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, 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; A. Pieczywok, *Training employees on risks in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1; M. Czuryk, *Supervision and Inspection in the Field of Cybersecurity* [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; A. Pieczywok, *Cyberspace as a source of dehumanisation of the human being*, „Cybersecurity and Law" 2023, no. 1; J. Kurek, *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022; M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1; P. Krawczyk, *Threats Posed by Cyberterrorism to Public Administration* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022; P. Krawczyk, J. Wiśnicki, *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, „Cybersecurity and Law" 2023, no. 1.

current Russian-Ukrainian war sheds new light on the issue, so in this paper we attempt to examine the situation, instruments and legal framework of cyber warfare in Poland and Hungary, using a comparative method.

## On military cyber defence in Hungary

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].

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[7]; 2) at the 2014 Wales Summit, NATO's cyber defence policy guidelines were adopted and cyber defence was included in the collective defence tasks[8]; 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 cyber-attack 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[9]; 4) at the 2018 Brussels Summit, it was declared that, while NATO is focused on

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

**7** For more on this, see idem, *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.

**8** *Wales Summit Declaration issued by NATO Heads of State and Government*, https://www.nato.int/cps/en/natohq/official_texts_112964.htm [access: 22.07.2023].

**9** Ibidem.

developing collective defence cyber capabilities, member states are building a full range of capabilities for deterrence and effective action[10].

To conclude this reflection, it is also worth pointing out that, in addition to cyber warfare, cyber diplomacy[11] is increasingly emerging as an instrument of state foreign policy, which can be defined as the use of diplomatic resources and procedures to promote national interests in cyberspace[12].

## Cyber warfare in Hungary

Two years ago, the Hungarian legislator adopted the National Security Strategy, which – among other things – required the Hungarian Defence Forces to build up the organisational, technical and human conditions for effective action against cyberattacks and hybrid warfare. At the same time, state, intelligence and civilian cyber defence capabilities were developed. In defining the tasks related to cyber warfare, the government, when drafting the national security strategy, also considered that it is no longer enough to protect organisations, objects, information centres and databases from external attacks, but that the Hungarian IT support force must also be able to identify the source of the attack and, not least, be able to launch a counter-attack.

Within this framework, an independent cyber defence unit was established within the Hungarian Defence Forces, which performs basic tasks in the defence of the Defence Forces and in securing the Defence Forces against attacks. The National Cyber Defence Institute, a special institute of the National Security Service, also performs partial tasks[13].

The Russia-Ukraine war makes the topic painfully topical, as the war in the neighbouring country also shows that it is not necessarily necessary to attack with firearms, but that services can be paralysed via the internet. In this context, telecommunications are becoming a target, and databases containing information of public interest and public utility, which may be linked to the

**10** *Brussels Summit Declaration issued by NATO Heads of State and Government*, https://www.nato.int/cps/en/natohq/official_texts_156624.htm [access: 22.07.2023].

**11** See G. Nyáry, *Cyber diplomacy: power, politics and technology in the fifth dimension of geopolitics* [in:] *Information and cybersecurity*, ed. B. Török, Budapest 2020, p. 332.

**12** For an introduction to cyber diplomacy processes, see L. Kerekes, *Waiting for Godot... Challenges of codifying a unified convention against cybercrime*, Debrecen 2021, p. 36–38.

**13** This shows that cyber warfare tasks are divided between several organisations, some military, some civilian, some intelligence and some state actors.

functioning of the state, may be at risk, and attacking, blocking or destroying them could cause chaos in society[14]. Equally targeted are government infrastructure, government communications, defence infrastructure, defence communications, priority industrial sites, and parts of the Hungarian banking system.

Among the legislative frameworks, it seems appropriate to mention Hungary's National Security Strategy, which states that „Hungary must be ready to address the risks and threats to national security, defence, law enforcement and disaster management that are increasingly emerging in cyberspace worldwide, to guarantee an adequate level of cyber security, to perform cyber defence tasks and to ensure the operation of national critical infrastructure"[15]. The Declaration of Principles is both a task definition and an infrastructure deployment and organisational commitment for public bodies. The National Military Strategy, which contains the following for our topic, concretises this state objective: 1) „[...] the growing number and damage potential of attacks against computer networks stands out. The characteristics of the cyber threat, which are different from traditional threats, call for a comprehensive review of our concepts of war and, where appropriate, modification; 2) [...] Such a threat is primarily cyber warfare, which is increasingly outpacing conventional weapons in terms of its potential to cause material damage and disrupt public order; 3) [...] the cyber defence of the Hungarian Defence Forces must be strengthened"[16].

In addition to outlining the tasks and competences of government bodies, the Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities and the National Cyber Security Strategy are worth highlighting, also due to their legal nature. The legislation places the field under the supervision of the National Directorate General for Disaster Management of the Ministry of the Interior in the state hierarchy. The legislation covers the infrastructures necessary for the maintenance of daily life (in a total of 10 sectors and 42 subsectors)[17], for which the supervisory authority also has the power to impose fines for breaches of information security requirements, as part of its powers of control.

**14** This includes health records, social security databases or pension databases.

**15** Government Decision 1035/2012 (II.21) on Hungary's National Security Strategy, point 31.

**16** Government Decision No 1656/2012 (XII. 20) on the adoption of the National Military Strategy of Hungary, points 33, 52, 82.

**17** These include the energy, health, transport and information technology sectors. For more information, see Annex 1 to Act CLXVI of 2012.

It is also appropriate to mention the Government Decision 1139/2013 on Hungary's National Cybersecurity Strategy, which on the one hand creates the cybersecurity environment, on the other hand defines the goals and tasks of the relevant actors, and provides a toolbox for the competent bodies and organisations, and under its auspices establishes the National Cybersecurity Coordination Council.

## The Cyberspace Defence Forces in Poland

The Polish Armed Forces are composed of 1) Land Forces; 2) Air Forces; 3) the Navy; 4) the Special Forces, and 5) the Territorial Defence Force. As a specialised component, the Cyberspace Defence Forces also form part of the Polish Armed Forces. They are competent for implementing a full range of activities in cyberspace, in particular when it comes to the proactive protection and active defence of cyberspace elements and resources which are of fundamental importance from the point of view of the Polish Armed Forces. This status arises from Art. 15 of the HDA[18]. The Cyberspace Defence Forces are not a specific type, but rather a component of the Polish Armed Forces; nevertheless, they are part of the Armed Forces, which means that the Constitution of the Republic of Poland also determines their position, which is further specified in the HDA. The fact that the legislator defines the Cyberspace Defence Forces as a specialised component means that they perform specific tasks which are essential from the point of view of state security, related to a domain requiring expertise in the use of ICT systems and their protection.

The object of activities of the Commander of the Cyberspace Defence Forces is defined in Art. 23 of the HDA. More specifically, the Commander supervises military units and organisational associations of the Cyberspace Defence Forces, and is subordinate, under Art. 23(1) of the HDA, to 1) the Minister of National Defence, whose domain of action covers supervising all activities of the Polish Armed Forces in times of peace[19] – until the appointment of the Commander-in-Chief of the Armed Forces; 2) the Commander-in-

**18** Homeland Defence Act of 11 March 2022 (Journal of Laws 2022, item 655, as amended).

**19** Art. 2(1) of the Act of 14 December 1995 on the Authority of the Minister of National Defence (consolidated text, Journal of Laws 2022, item 1438). See also M. Karpiuk, *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1, p. 87.

Chief of the Polish Armed Forces upon their appointment and assumption of command of the Polish Armed Forces. For the duration of war, the President of the Republic of Poland, at the request of the Prime Minister – as stipulated in Art. 134(4) of the Constitution of the Republic of Poland – appoints the Commander-in-Chief of the Armed Forces[20]. Upon his/her appointment by the President of the Republic of Poland and the assumption of command of the Polish Armed Forces, the Commander of the Cyberspace Defence Forces becomes subordinated to them, and this shall continue for the duration of a war and, therefore, as stipulated in Art. 2(2) of the HDA, for the duration of military operations conducted in the territory of Poland, the beginning and end of which is defined by the President of the Republic of Poland, by way of a decision issued at the request of the Council of Ministers.

The scope of activities of the Commander of the Cyberspace Defence Forces is defined in Art. 23(2) of the HDA, which includes in particular: 1) implementing the development programme of the Polish Armed Forces; 2) programming, planning, organising, conducting and supervising the conduction of training courses falling within the scope of the duties of the Commander of the Cyberspace Defence Forces for the benefit of subordinate military units and organisational associations, organisational sections and units, as well as other institutions, bodies and entities, based on concluded agreements; 3) planning and organising the mobilisation, operational development and use of the Cyberspace Defence Forces; 4) constructing, maintaining and protecting infrastructure, as well as protecting information in cyberspace[21]; 5) conducting activities and operations in cyberspace; 6) providing support for military operations conducted by the Polish Armed Forces along with operations within the allied and coalition system; 7) cooperating with other bodies and entities in matters regarding national defence; 8) managing and conducting inspections of subordinate military units and organisational associations[22]. Inspections are conducted to assess the activity of the inspected unit based on established facts and using adopted inspection criteria. If any irregularities are found, the purpose of the inspection

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

**21** See also M. Nowikowska, *Protection of Critical Infrastructure in Cyberspace* [in:] *The Public Dimension of Cybersecurity*..., p. 79–92.

**22** See also: M. Nowikowska, *Ocena funkcjonalności systemu kontroli w Siłach Zbrojnych RP*, Warszawa 2018, p. 40; eadem, *Działalność kontrolna w Siłach Zbrojnych RP* [in:] *Prawo wojskowe*, eds. W. Kitler, D. Nowak, M. Stepnowska, Warszawa 2017, p. 491–507.

is to determine their scope, causes and effects, as well as the persons responsible for their occurrence, and finally to formulate recommendations aimed at removing the irregularities[23].

Article 11(3) of the HDA stipulates that the Polish Armed Forces may participate in combating natural disasters and eliminating their consequences, as well as anti-terrorist actions, actions in the field of property protection, search actions, and actions to save or protect human health and life, actions to protect and defend cyberspace, in clearing areas of explosives and hazardous materials of military origin and their disposal, as well as in implementing tasks in the field of crisis management. The legislator stipulates that the Polish Armed Forces may participate in the protection and defence of cyberspace. These duties should be entrusted to the Cyberspace Defence Forces as a specialised formation competent for safeguarding cybersecurity.

The issue of the use of the Cyberspace Defence Forces outside the national territory has not been expressly regulated. The use of the Polish Armed Forces (including the component competent for safeguarding cybersecurity) outside the national territory means the presence of military units outside that territory to participate in 1) an armed conflict or to strengthen the forces of an allied state or states; 2) a peacekeeping mission; 3) an action to prevent acts of terrorism or their consequences; 4) the evacuation of Polish citizens when there is a need to protect their life or health, from a state that is not an EU Member State, a Member State of the European Economic Area or a signatory to the North Atlantic Treaty[24]. As regards using the Cyberspace Defence Forces outside the national territory, the legislator has made no mention of the effect of such actions. In the case of offensive actions in cyberspace, there is no need for military units to be deployed there to achieve an effect outside the national territory. In order to destroy a target in another country, the presence of the Cyberspace Defence Forces is not always required, especially since cyberspace has a global reach.

The Commander-in-Chief of the Armed Forces has competence for commanding military units and organisational associations of the

**23** Art. 3 of the Act of 15 July 2011 on Inspections in Government Administration (consolidated text, Journal of Laws 2020, item 224). See also M. Nowikowska [in:] *Ustawa o kontroli w administracji rządowej. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Nowikowska, Warszawa 2021, p. 10–19.

**24** Art. 2(1) of the Act of 17 December 1998 on the Principles of Use or Stay of the Polish Armed Forces outside the National Territory (consolidated text, Journal of Laws 2021, item 396, as amended).

Armed Forces of the Republic of Poland, excluding the military units and organisational associations of the Armed Forces of the Republic of Poland that are subordinated to the Commander of the Cyberspace Defence Forces. This exclusion arises from Art. 20(1)(5) of the HDA. Accordingly, the Commander of the Cyberspace Defence Forces has competence for commanding the Cyberspace Defence Forces.

Pursuant to Art. 134(1–2) of the Constitution of the Republic of Poland, the President of the Republic of Poland shall be the supreme representative of the Armed Forces of the Republic of Poland. In times of peace, the President shall exercise command over the Armed Forces through the Minister of National Defence. This also applies to Cyberspace Defence Forces.

The task of the Cyberspace Defence Forces – a uniformed and armed formation – is to ensure security in cyberspace[25]. This competence applies to cyberspace security in the military dimension.

## Conclusion

The issue of safeguarding security in cyberspace should also be perceived in military terms. Protecting against, countering and recovering from cyber threats is a challenge for the military domain, which must respond to any emerging incidents that exert an increasingly severe impact. The cyber-threat landscape is dynamic in nature, as should be cyberspace defence. As activities in cyberspace can lead to armed conflicts, the armed forces must have a cyberspace defence capability, including the capability of ensuring the stability of cyberspace in the military dimension, which, as an operational domain, is constantly under attack.

In the case of the Polish Armed Forces, the objective is to strengthen their operational capabilities for deterrence and defence against security threats. The particular focus here should be on increasing the level of mobility and technical modernisation. Emphasis is placed, *inter alia*, on obtaining operational capabilities to conduct wide-ranging military operations in cyberspace, developing the Cyberspace Defence Forces and building capabilities for space operations and information operations. Other strategic objectives of the state are to increase resilience to cyber threats and to improve information

**25** A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, op. cit., p. 36.

protection in the military sector. This objective is to be achieved by increasing the level of resilience of the information systems used in the military domain by achieving the ability to effectively prevent, combat and respond to cyber threats, as well as by conducting a wide range of military operations in cyberspace[26].

The Armed Forces of the Republic of Poland, as a fundamental element of the state defence system, are to engage in cyberspace operations to the same degree as in the air, on land and at sea, during peace and war, and in crises. Therefore, military capabilities in cyberspace must include threat intelligence, protecting and defending ICT networks and systems, and combating sources of cyber threats[27].

To sum up, cyber warfare is one of the major challenges of our time, which the public sector (both civilian and defence, as well as through academic backbone institutions) needs to address both actively and proactively. It is also clear that our systems are vulnerable, and therefore there is at least as much state responsibility to be identified in terms of the technical, procedural, legal and infrastructural conditions for cyber security as there is for responding to cyber security incidents that occur. Cyber terrorism can be identified as a serious threat: while state-sponsored cyberattacks are predictable, guerrilla-type incidents can be assessed as a serious source of uncertainty, against which international/supranational action cannot be delayed. The legal framework underlines that Hungary is on the right track in this respect, but there is still work to be done and not a little of it.

To conclude, it should be stressed that the armed forces have been entrusted with special tasks in the sphere of defence, as their duty is to protect the state against external threats, including armed aggression. Such threats may also take the form of cyber-attacks[28].

## Bibliography

Bencsik A., Karpiuk M., *Cybersecurity in Hungary and Poland. Military aspects*, „Cybersecurity and Law" 2023, no. 1.

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

**26** *Cybersecurity Strategy of the Republic of Poland*, Warszawa 2020, p. 18–20.

**27** Cybersecurity Strategy of the Republic of Poland 2019–2024, Appendix to Resolution No. 125 of the Council of Ministers of 22 October 2019 (M.P. 2019, item 1037), p. 19.

**28** M. Karpiuk, *Activities of the Polish Armed Forces in Cyberspace and Their Constitutional Status*, „Przegląd Prawa Konstytucyjnego" 2023, no. 3, p. 286.

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., *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.
Czuryk M., *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2.
Kurek J., *Operational Activities in the Field of Cybersecurity* [in:] *Cybersecurity in Poland. Legal Aspects*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.
Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Rocznik Nauk Społecznych" 2023, no. 2.
Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Activities of the local government units in the scope of telecommunication*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *Activities of the Polish Armed Forces in Cyberspace and Their Constitutional Status*, „Przegląd Prawa Konstytucyjnego" 2023, no. 3.
Karpiuk M., *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2.
Karpiuk M., *Cybersecurity as an element in the planning activities of public administration*, „Cybersecurity and Law" 2021, no. 1.
Karpiuk M., *Organisation of the National System of Cybersecurity: Selected Issues*, „Studia Iuridica Lublinensia" 2021, no. 2.
Karpiuk M., *Tasks of the Minister of National Defence in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Karpiuk M., *The executive agency as a legal organisational form of implementing cybersecurity tasks*, „Cybersecurity and Law" 2023, no. 1.
Karpiuk M., *The Local Government's Position in the Polish Cybersecurity System*, „Lex Localis – Journal of Local Self-Government" 2021, no. 3.
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.
Karpiuk M., Kelemen M., *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2.
Kerekes L., *Waiting for Godot... Challenges of codifying a unified convention against cybercrime*, Debrecen 2021.
Krawczyk P., *Threats Posed by Cyberterrorism to Public Administration* [in:] *The Role of Cybersecurity in the Public Sphere – The European Dimension*, eds. K. Chałubińska-Jentkiewicz, I. Hoffman, Maribor 2022.
Krawczyk P., Wiśnicki J., *Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine*, „Cybersecurity and Law" 2022, no. 2.
Krawczyk P., Wiśnicki J., *Russia's social-impact operations in the context of cognitive warfare in Ukraine in 2022*, „Cybersecurity and Law" 2023, no. 1.
Nowikowska M. [in:] *Ustawa o kontroli w administracji rządowej. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Nowikowska, Warszawa 2021
Nowikowska M., *Działalność kontrolna w Siłach Zbrojnych RP* [in:] *Prawo wojskowe*, eds. W. Kitler, D. Nowak, M. Stepnowska, Warszawa 2017.

Nowikowska M., *Ocena funkcjonalności systemu kontroli w Siłach Zbrojnych RP*, Warszawa 2018.
Nowikowska M., *Protection of Critical Infrastructure in Cyberspace* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.
Nowikowska M., *The right to privacy in cyberspace* [in:] *Human Rights as a Guarantee of Smart, Sustainable and Inclusive Growth*, eds. I. Florek, I. Laki, Budapest 2022.
Pieczywok A., *Cyberspace as a source of dehumanisation of the human being*, „Cybersecurity and Law" 2023, no. 1.
Pieczywok A., *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2.
Pieczywok A., *Training employees on risks in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.
Tóth T., *Introducing the NATO Cyber Defence Centre of Excellence*, „National Security Review" 2018, no. 4.
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.

## Status prawny cyberwojsk na Węgrzech i w Polsce. Zarys problematyki

**Streszczenie**

Zadania mające na celu zapewnienie bezpieczeństwa w cyberprzestrzeni dotyczą nie tylko sfery cywilnej, lecz także wojskowej. Cyberprzestrzeń jako domena operacyjna, podobnie jak i inne środowiska, jest narażona na zagrożenia, w tym te o charakterze destrukcyjnym, destabilizującym funkcjonowanie państwa czy jego instytucji. Ze względu na konieczność zapewnienia cyberbezpieczeństwa w wymiarze militarnym poszczególne państwa tworzą cyberwojska mające zapewniać stabilność cyberprzestrzeni, która jest narażona na ciągłe ataki. Cyberobrona w państwie cyfrowym, gdzie również zadania o charakterze wojskowym są wykonywane z wykorzystaniem systemów teleinformatycznych, musi stanowić priorytet nie tylko polityki obronnej poszczególnych państw, lecz także międzynarodowej.

**Słowa kluczowe:** cyberwojska, cyberprzstrzeń, cyberbezpieczeństwo