Oksana Evsyukova*
Mirosław Karpiuk**
Miroslav Kelemen***

Cyberthreats in Ukraine, Poland and Slovakia

Abstract

This article focuses on cyberthreats in Ukraine, Poland and Slovakia. As the ICT system in a digital state plays an important role, states are obliged to ensure their adequate protection. Interference with the proper functioning of such systems can have far-reaching consequences, potentially leading to the paralysis of specific economic sectors. The continually emerging cyberthreats, their intensity and types trigger the need to constantly monitor the phenomena occurring in cyberspace. With such monitoring cyberattacks can be countered and their destructive outcomes avoided. The article indicates, *inter alia*, the types of cybersecurity incidents and their frequency.

Key words: cybersecurity, cyberspace, cyberthreats

* Assoc. Prof. Oksana Evsyukova, Department of Public Administration, Management of Innovative Activities and Consulting, National University of Life and Environmental Sciences of Ukraine, e-mail: oksana_evsyukova@yahoo.com, ORCID: 0000-0002-1299-6955.

** 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.

*** Prof. Miroslav Kelemen, PhdSc., Vice-Rector for Education, Technical University of Kosice, e-mail: miroslav.kelemen@tuke.sk, ORCID: 0000-0001-7459-927X.

Introduction

Modern countries and societies are, to a large extent, digitalised and rely on ICT systems to perform some strategic functions. These systems are responsible, *inter alia*, for ensuring the stability of a state and its economy. As such, they must be adequately protected. In addition, they play a very important role in society. For this reason, their reliability and security must be viewed as a priority by entities in charge of the operation of these systems, both in the public and private sectors[1]. It is, therefore, indispensable for these entities to ensure the cybersecurity of such ICT systems. Cybersecurity is defined as the resilience of information systems (while an information system is an ICT system together with the electronic data processed in it) against any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems[2]. Cybersecurity is a type of

1 A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 89–90.

2 Art. 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (consolidated text, Journal of Laws 2023, item 913, as amended), hereinafter referred to as „the NCSA". Regarding cybersecurity, see also: M. Czuryk, *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2; 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; A. Pieczywok, *The use of selected social concepts and educational programmes in counteracting cyberspace threats*, „Cybersecurity and Law" 2019, no. 2; M. Adamczyk, M. Karpiuk, U. Soler, *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4; M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, no. 2; M. Czuryk, *Supervision and Inspection in the Field of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022; A. Pieczywok, *Cyberspace as a source of dehumanization of the human being*, „Cybersecurity and Law" 2023, no. 1; K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, no. 2; M. Czuryk, *Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity*, „Cybersecurity and Law" 2019, no. 2; D. Prokopowicz, M. Matosek, *Importance and Security of Information Provided by the Internet in the Context of the Development of Economic Entities in Poland*, „International Journal of New Economics and Social Sciences" 2017, no. 2; M. Czuryk, *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, 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; K. Chałubińska-Jentkiewicz, *Cyberodpowiedzialność*, Toruń 2019; M. Karpiuk, *Tasks of the Minister of National Defense in the area of cybersecurity*, „Cybersecurity and Law" 2022, no. 1.

generic security[3], with prevention being an important step to ensure security (thus also cybersecurity)[4]. A cybersecurity threat is defined in Art. 2(17) of the NCSA as a potential cause of an incident, and an incident, according to Art. 2(5) of the NCSA, is an event which has or may have an adverse effect on cybersecurity.

While technological progress enables more efficient and faster task performance and facilitates communication, it also involves certain threats. Some cyberthreats can disrupt the proper functioning of a state. Because cyberattacks can cause substantial losses, ensuring cybersecurity has become indispensable, and this is where money should not be spared. Failure to adequately protect ICT systems can generate exorbitant costs when a cyberattack occurs.

Most of society's activities have moved online. As a result, ensuring digital security is a fundamental duty of public authorities. The functioning of the information society relies heavily on ICT systems, which are vulnerable to disruptions affecting society. Threats to its functioning have increasingly serious consequences, and cyberattacks can be used to exert political or economic pressure. The huge amount of information and the dynamic development of information technologies are changing all aspects of our social, cultural, economic or political life[5].

Cyberspace is where public, private, social and economic activities are conducted. It is used for providing different kinds of services and for communication. As cyberspace is highly important for the state and society, the duty to protect it rests with public and private institutions. Therefore, protection against cyberthreats must be considered a priority in state policies and the duty of those in charge of ensuring the security of ICT systems[6].

It is a public task to ensure the security of information systems, but the fact that this is an extremely dynamic area makes it challenging. The development

3 D. Tyrawa, *Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane*, „International Journal of Legal Studies" 2023, no. 1, p. 18.

4 M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4, p. 122.

5 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 145.

6 M. Karpiuk, M. Kelemen, *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2, p. 71.

of new technologies requires the search for new solutions to ensure the security of activities carried out in cyberspace[7].

Cyberthreats in Ukraine

The creation of a digital state in Ukraine has recently become particularly relevant, as evidenced not only by the documents adopted by the Government of Ukraine but also by concrete actions aimed at implementing the ambitious idea of building the most convenient and secure state in the world, from the perspective of interaction between citizens and the state. However, the war in Ukraine has created a complex network of risks, primarily related to a significant number of cyberthreats in Ukrainian cyberspace across various spectrums. In today's circumstances, this issue is not a new challenge for the Ukrainian state and remains relevant due to the continuation of Russian aggression on the Ukrainian territory.

It is worth emphasising that 2018 was a year of positive steps towards the affirmation of cybersecurity and cybersovereignty in Ukraine. The adoption of Ukraine's Information Security Doctrine in 2017 laid the foundation upon which the state could begin to rebuild its activities in this field, based on the unity of strategic intent and coordination of actions among various government bodies. However, there remain significant strategic challenges and threats in the realm of information security that require immediate attention. Thanks to the systematic efforts of Ukrainian government structures taken between 2014 and 2019, it was possible to significantly reduce Russia's capabilities in spreading its destructive narratives within Ukraine's territory. This was facilitated by the restriction of Russian television channels and Russian media content (TV series, movies), increased control over printed literature containing expressions and narratives that pose a threat to national security, the imposition of economic sanctions (which further limited the activities of certain Russian social media platforms), targeted expulsion of employees of Russian propaganda media from the country, and so on.

However, the remaining key issue is strategic disinformation campaigns carried out by the aggressor, utilising its entire arsenal of tactics and means

7 I. Hoffmam, M. Karpiuk, *The local self-government's place in the cybersecurity domain. Examples of Poland and Hungary*, ibidem, no. 1, p. 173.

in conducting information warfare. Russia has developed a well-defined propaganda system that aligns with the clear political will of its leadership. The main objectives of such campaigns have been known and have changed little over the years, including discrediting the Ukrainian government, sowing discord between the authorities and citizens as if they were antagonistic entities, discrediting Ukraine on the international arena, legitimising the annexation of Crimea and military terrorist entities, and inciting internal political turmoil (also by exploiting tensions between Ukraine and some neighbouring states). The onset of Russian intervention in 2022 in the Ukrainian territory has created new opportunities for pursuing their hidden intentions, including cyberthreats, which are an integral component of any hybrid conflict.

To understand the above, it is worth considering examples of cyberthreats in Ukraine. For instance, back in March 2014, „New York Times" reported that malicious software called „Snake" had infiltrated the office of the Prime Minister of Ukraine and several remote embassies, along with the start of anti-government protests in Ukraine. At the end of 2013 and the beginning of 2014, ESET also published research documenting attacks on military facilities and mass media, which were named „Operation Potao Express". As before, a self-proclaimed cybergroup known as „Cyber Berkut" carried out DDoS attacks and web defacements without causing any significant harm. However, this created a lot of confusion, which was meaningful during the conflict. For example, at the beginning of the conflict, Russian soldiers effortlessly gained control over the telecommunications networks of Crimea and the region's only internet station, leading to an information blackout. Attackers used access to the mobile network to identify participants in anti-Russian protests and to send them text messages reading as follows: „Dear subscriber, you are registered as a participant in mass riots". After isolating Crimea's communication, the attackers also hacked the mobile phones of members of the Ukrainian Parliament, making them unable to effectively respond to the invasion. In other words, disinformation campaigns were fully deployed. The critical aspect of the situation was that state institutions became the primary target of the attack.

Let us consider an attack on Ukraine's energy system as a cyberthreat example. On 23 December 2015, electricity was suddenly cut off for approximately half of the residents of Ivano-Frankivsk, a city in Western Ukraine. It is now understood that this attack was sponsored by state-backed Russian hackers. The initial attacks began more than six months before the power outage when employees of three electricity distribution centres

opened a malicious Microsoft Office document with a macro designed to install malicious software called Black Energy. The criminals obtained remote access credentials to the supervisory control and data acquisition (SCADA) network and gained control over the substation control elements to initiate the automatic circuit breaker switch-off. Afterwards, the attackers locked these control panels to prevent remote switching of the breakers to restore power. In addition, the perpetrators deployed malicious „wiper" software to lock computers used for network management. They simultaneously carried out a Telephony Denial of Service (TDoS) attack, blocking customer support phone numbers to deny access to customers attempting to report the outages. Almost a year later, a similar attack was executed in Kiev. This time, the malicious software responsible was Industroyer/Crash/Override, and was much more sophisticated. The malware was designed with modular components that could scan the network for SCADA controllers and communicate in their language. The attack was not linked to BlackEnergy or to the well-known KillDisk tool, but the identity of the perpetrators remained uncertain.

In 2017, as part of Russian campaigns aimed at undermining the Ukrainian statehood, a series of cyberoperations were carried out against Ukraine. The main ones included „BugDrop" (June 2016–March 2017), „WannaCry" (also known as „WannaCwt", June 2017), and „NotPetya" (also known as „Petya.A", „Petya", 27–30 June 2017). The objectives of these cyberoperations were to gather confidential information about critical infrastructure objects, government agencies, and international offices, including human rights organisations, political parties, and influential media, including those in temporarily occupied territories in the Donetsk and Luhansk regions and the Autonomous Republic of Crimea, as well as to disrupt the functioning of management systems in large companies, energy and transportation infrastructure facilities, and banking institutions to weaken the Ukrainian economy. According to assessments by cybersecurity experts from the American research company „CyberX", as a result of the „BugDrop" operation, hacker groups under Russian control infiltrated the networks and systems of international (especially human rights) organisations operating in the temporarily occupied territories in the Donetsk and Luhansk regions, energy infrastructure facilities, research institutions, some influential media, using „unconventional" methods to penetrate computer networks and to obtain confidential information circulating within government agencies and critical infrastructure objects, including energy infrastructure. The result of the „WannaCry" cyberoperation was the infection and disruption of approximately

300 000 computers in around 150 countries, with hacker groups managing to fraudulently obtain funds ranging from 1 to 4 billion US dollars, according to various estimates. Western expert institutions attribute the responsibility for the „WannaCry" cyberoperation to Russia and North Korea . The „NotPetya" cyberoperation, which took place between 27 and 30 June 2017, was directed against Ukraine and was anti-Ukrainian in nature. Western governments now publicly acknowledge that the Russian Federation was responsible for this attack. They also recognise that Russia does not intend to limit its unlawful activities in cyberspace. In 2017, Russia attempted to attack the energy infrastructure of the United States and the United Kingdom. In 2018, it consistently expanded the geographic range and the nature of its cyberattacks on Western governments, targeting the United States , Germany, the United Kingdom, and the Netherlands, among others. A powerful cyberattack that had been detected in advance was being prepared against Ukraine. International research organisations and Ukrainian law enforcement agencies jointly uncovered a massive infection of network devices, using malicious software called VPNFilter. According to the SBU (Security Service of Ukraine), this attack was being prepared for cyberespionage and cybersabotage purposes, including targeting national critical infrastructure facilities. The detection and prevention of this attack was possible thanks to the year-long efforts in the field of cybersecurity in Ukraine, including assistance from NATO. In 2017, the first stage of the NATO Trust Fund , the main organisational and technical goal of which was the development of a network of cybersecurity situational centres, was successfully completed. Within this stage, the following centres were opened within the structure of entities of the national cybersecurity system: the Security Service of Ukraine (the Cybersecurity Assurance Situation Centre), the National Bank of Ukraine (CERT), and the State Special Communications and Information Protection Service (the Cyber Threat Response Centre).

In 2022, when political tension escalated before the war, many Ukrainian government websites were damaged, and systems were infected with malicious software disguised as ransomware attacks. Some components of these attacks mirrored the past. The malicious software was not ransomware; it was simply a sophisticated wiper, as seen in the NotPetya attacks. Additionally, numerous false flags were left, suggesting that this could be the work of Ukrainian or Polish hackers.

The following events serve as recent examples of a large-scale cyberattack. On 12 December 2023, the largest telecommunications operator in Ukraine,

Kyivstar, experienced a massive outage. Mobile communication and Internet services disappeared for Kyivstar subscribers across the country, and users could not connect to networks of other operators within the scope of domestic Ukrainian roaming. Additionally, the Kyivstar website and application ceased to function. Communication was disrupted for 24 million subscribers, prompting the National Bank of Ukraine to recommend that banks establish backup communication channels following the cyberattack on Kyivstar (source: RBC Ukraine, December 22, 2023). Failures occurred in all equipment that used the Kyivstar communication, leading to serious infrastructure problems throughout Ukraine. The President of Kyivstar, Alexander Komarov, called this „the world's largest cyberattack on telecom infrastructure". The attack occurred amidst the Russian invasion of Ukraine. The Russian hacker group Solntsepek claimed responsibility for the attack. Additionally, another Ukrainian bank, Monobank, experienced an attack on its computing system on 19 January 2024, with over 50 million meaningless requests that overloaded the system. However, on 20 January 2024, the most powerful DDoS attack was repelled, confirming the excellent and skilled work of the Ukrainian IT army.

Since Russian troops are targeting Ukraine, and distributed attacks such as Distributed Denial of Service (DDoS) occasionally disrupt the operations of Ukrainian government websites and financial service providers, many are talking about readiness for a cyberconflict. However, any organisation (particularly governmental institutions) should always be prepared for attacks from any direction. In such conditions, it is quite important to know what to pay attention to when the risk of an attack is increasing. Therefore, it is worth reviewing the history of known or anticipated actions of the Russian state in cyberspace to assess what types of activities to expect and how the state, businesses, and civil society can prepare for these.

As the conflict escalated into Russia's intervention, it became clear that the standard Russian conflict scenario was in play, i.e., deflect, confuse, deny, and attempt to divide. On 15 February 2022, a series of major DDoS attacks were carried out on Ukrainian government and military websites, and the three largest banks in Ukraine. The White House has already declassified some intelligence and attributed responsibility for the attacks to the Russian GRU. The war began on 24 February 2022. Sophos continuously updates information on the development of cyberattacks as they evolve.

It is worth mentioning that the information war that Russia has been waging against Ukraine for many years is aimed at both its own residents and the citizens of our state. Currently, this has resulted in Ukrainians being

very adept at recognising fake news and sources with pro-Russian rhetoric. Significantly, the majority of Ukrainians consciously choose verified and official sources. The information policy is based on a key principle – the government must be transparent and open when communicating with the people, even though there is sometimes concealment of true and accurate information from the Ukrainian government. An example of the most widely spread fake news intended to cause panic among Ukrainian citizens and reassure Russians is the following case. In late August 2022, the Russian publication „New Inform" spread the news with the headline: „The Washington Post: Zelensky decided to resign and leave the territory of Ukraine in the early days of the special operation". This information was also disseminated by Russian Yandex, RT, Gazeta.ru, and dozens of other channels. It claimed that journalists from The Washington Post had found out that the President of Ukraine was planning to leave the country on the eve of military actions. In reality, the original article mentioned that Western leaders were merely advising Zelensky to leave Kyiv. This should be interpreted as a deliberate distortion of the quote („difficulties in translation into Russian"), and was premeditated as an information influence.

In summary, regardless of whether the situation escalates, undoubtedly, cyberoperations will undoubtedly continue. Ukraine has been under a constant barrage of attacks with varying degrees of intensity since the fall of Viktor Yanukovych in 2014. This implies the continuation of previous behaviour, leading up to the conflict, and makes DDoS attacks a potential indicator of the inevitable conduct during the war. It is worth realising that information warfare is how Russia may attempt to control the rest of the world's reaction to actions in Ukraine or any other target of its attack. From a global perspective, it should be expected that a whole range of „patriotic" freelancers in Russia, including extortionists, phishing writers, and botnet operators, will be even more zealous than usual in targeting what is believed to be threats to their country.

It is unlikely that Russia will directly attack NATO members and risk invoking Art. V. However, its recent actions in curbing criminals operating from the Russian territory and their partners in the Commonwealth of Independent States (CIS) are likely to cease and, instead, we will see threats multiplying. While layered information security should be an everyday task even in ordinary times, it is particularly crucial when an increase in the frequency and severity of attacks is anticipated.

In order to strengthen the protection of the homeland's cyberspace, it is deemed necessary to enhance the capabilities and to activate the interaction of competent law enforcement agencies in the following directions: 1) detecting, preventing, and localising (terminating) special information operations by the aggressor country against Ukraine; 2) identifying facts and attempts to manipulate public consciousness, including the dissemination of false, incomplete, or biased information, fomenting panic through mass media, including the Internet; 3) monitoring the impact on the domestic media market of processes occurring in information, political, economic, social, and other spheres, in order to forecast changes taking place in them, as well as potential threats to information security, and to ensure timely response; 4) strengthening control over the activities of foreign information structures and their officials, primarily Russia, and taking effective measures to prevent their anti-Ukrainian information activities; 5) taking additional measures aimed at blocking the dissemination in the media and online space of materials containing calls to undermine the state sovereignty, and territorial integrity of Ukraine, fuelling interethnic and interfaith conflicts, and promoting war.

It is important for Ukrainians to remember that disinformation and propaganda will soon reach their peak, so it is necessary to systematically monitor the enemy, block disinformation, and keep an eye on anything unusual in our networks as the war flares up and subsides, even when it comes to an end.

Cyberthreats in Poland

In 2022, according to CERT Poland, 322 479 cybersecurity incidents were reported, but some of them were eventually not recognised as incidents. Based on its classification criteria, CERT Poland selected 115 164 reports and recorded 39 683 cybersecurity incidents. In 2022, a 34% increase in the number of cybersecurity incidents registered was observed compared to 2021. The number of all reported cases increased by nearly 178%, and the number of those specifically related to incidents by more than 75%[8]. CERT Poland performs the tasks assigned to CSIRT NASK.

8 *Raport roczny z działalności CERT Polska 2022. Krajobraz polskiego Internetu*, Warszawa 2023, p. 36.

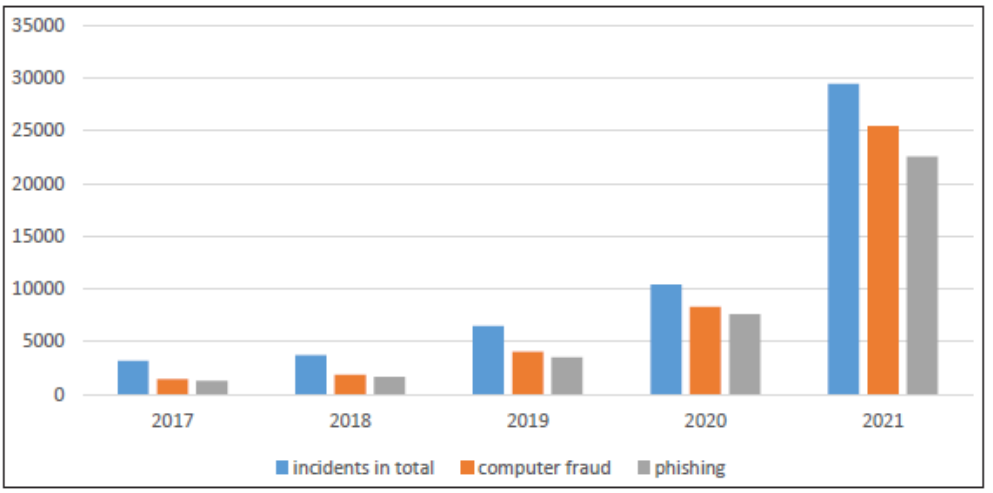
Under Art. 2(3) of the NCSA, CSIRT NASK is the Computer Security Incident Response Team operating at the national level, run by the Research and Academic Computer Network – National Research Institute. As stipulated in Art. 26(3) of the NCSA, NASK CSIRT's tasks include: 1) monitoring cyberthreats and incidents at the national level; 2) estimating risks related to the identified cyberthreats and incidents, including dynamic risk analysis; 3) providing information on incidents and risks to entities of the national cybersecurity system; 4) issuing announcements on the identified cyberthreats; and 5) responding to the reported incidents[9]. As the cyberthreat landscape is dynamic, measures to protect against these threats must keep pace with it[10]. This also applies to CERT Poland, the computer security incident response team.

Among incidents recorded by CERT Poland in 2022, those involving computer fraud, in particular phishing, were the most prevalent. 25 625 incidents classified as phishing were recorded, accounting for 64% of all incidents handled in 2022. The most popular type of phishing involved using the image of a courier company, InPost, with 5119 incidents recorded, followed by the social networking site Facebook, with 4370 incidents recorded. Malware was the second most frequently reported type of incident in 2022. Based on 15 433 reports, 3409 incidents of this type were eventually recorded. Among the recorded incidents, 2607 involved Flubot malware. The third type of incidents common in 2022 involved hacking, e.g., IT systems and e-mail accounts, with 354 incidents recorded. This apparently low number of recorded incidents results from the fact that hacking is often reported along with the phishing domain, which ultimately leads to its being commonly classified as phishing. Finally, 308 incidents classified as offensive and illegal content were recorded in the year under consideration[11].

9 See also M. Nowikowska [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 200.

10 A. Bencsik, M. Karpiuk, *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2, p. 28.

11 *Raport…*, p. 36.



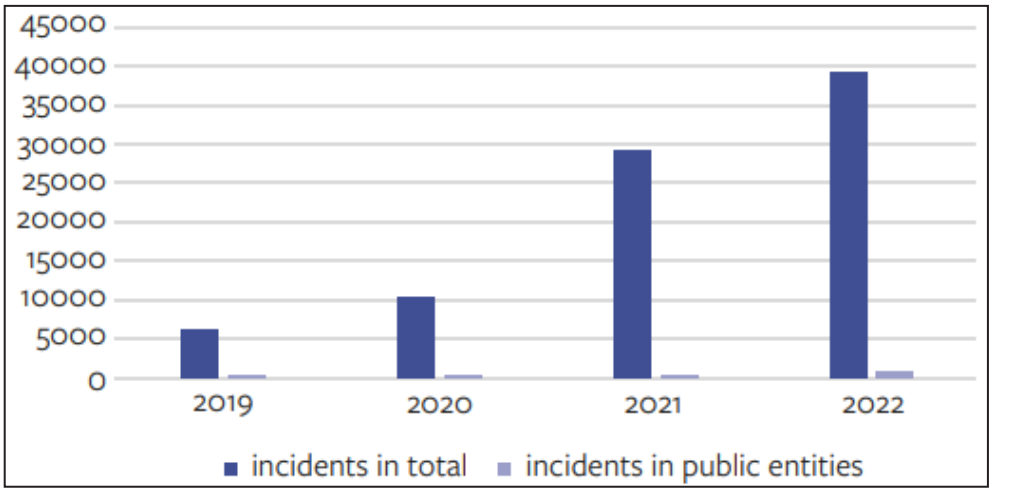
Source: M. Karpiuk, *Computer fraud*, „Cybersecurity and Law" 2023, no. 2, p. 192.

Figure 1. Incidents involving computer fraud recorded by CERT Poland in 2017–2021

CERT Poland also handles serious incidents, i.e., those which, under Art. 2(7) of the NCSA, cause or are likely to cause a severe deterioration in the quality or interruption of the continuity of an essential service[12]. In 2022, it handled 30 incidents classified as serious. More specifically, 21 serious incidents affected the banking sector, five in the energy sector, three in the healthcare sector, and one in the transport sector[13].

In 2022, CERT Poland handled 937 incidents in public entities. Under Art. 2(9) of the NCSA, an incident in a public entity causes or is likely to cause a severe deterioration in the quality or interruption of a public task implemented by that entity[14]. As part of incidents in public entities, 547 incidents were handled in the public administration sector, 134 in the education sector, and 81 in the digital infrastructure sector[15].

12 See also G. Szpor [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019, LEX/el., Art. 2.
13 *Raport*..., p. 37.
14 See also B. Kuś [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022, p. 25–26.
15 *Raport*..., p. 37.



Source: M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, „Prawo i Więź" 2023, no. 4, p. 20.

Figure 2. Incidents in public entities recorded by CERT Polska in 2019–2022

Incidents affecting the public administration sector were the most frequent among those classified as incidents in public entities. Modern public administration strives to set up stable and predictable institutions but should also be flexible enough to adapt to diversified social challenges. These institutions should be open to dialogue with society and keen on proposing new solutions and improving their services. The concept of modern administration is directly linked to its modernisation, this being one of the basic indicators of public action in all developed countries[16]. Modern administration must take into consideration the premises enabling the protection of cybersecurity.

Cybersecurity of e-administration includes adequately protecting its resources, i.e., digital content, ICT systems, devices, and content transmission through these systems. For such protection to be effective, it is necessary to build user awareness, as users are the targets of potential cyberattacks[17]. At the same time, it should be emphasised that humans, forming part of the social

16 J. Blicharz, L. Zacharko, *Kilka refleksji na temat rozumienia nowoczesnej administracji publicznej*, „Gubernaculum et Administratio" 2022, no. 1, p. 10.

17 P. Romaniuk, *Kształtowanie administracyjnoprawnych warunków służących do budowy cyberbezpieczeństwa w administracji publicznej*, „Cybersecurity and Law" 2023, no. 2, p. 92.

system, are currently the weakest link in the cybersecurity system in public administration, rather than its infrastructure capabilities or solutions [18].

In public administration, attempts have been made for many years to develop e-services. These include making a wide range of services available by electronic means, increasing the efficiency of public administration through implementing interoperable IT solutions, making available public sector information from registers to extend service offerings, and mutually recognising ICT solutions and tools[19]. These measures must also aim to counter cyberthreats occurring in public administration.

Public administration should take into consideration the principle that an adequate level of cybersecurity needs to be ensured for any new digital investment[20].

Countering cyberthreats requires cybersecurity planning. This allows for coordinated measures to be taken, enabling the adequate, timely and harmonious implementation of the objectives set for the relevant authorities in a structured and continuous manner. This applies particularly when multiple entities are involved[21].

Cyberthreats in Slovakia

Building the capabilities of the Slovak Republic in the field of cybersecurity is the top priority for the National Security Office. The National Centre for Cybersecurity SK-CERT (abbreviated as NCKB SK-CERT) was established on 1 September 2019. It was set up to develop capabilities in dealing with cybersecurity incidents at the national level, to expand and share knowledge and experience in this area, and to pursue active cooperation with the public, professional organisations, and the academic sector[22].

18 E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, ibidem 2022, no. 1, p. 218.

19 P. Romaniuk, *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, „Studia Prawnoustrojowe" 2022, no. 58, p. 442.

20 K. Gawkowski, *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2, p. 104.

21 M. Karpiuk, *Cybersecurity as an element in the planning activities of public administration*, ibidem 2021, no. 1, p. 46.

22 R. Konečný. *The National Centre for Cybersecurity SK-CERT*, https://www.nbu.gov.sk/2019/09/09/narodny-bezpecnostny-urad-1-septembra-2019-zriadil-narodne-centrum-kybernetickej-bezpecnosti-sk-cert/index.html [access: 2.02.2024].

The National Centre for Cybersecurity SK-CERT, the Competence and Certification Centre for Cybersecurity (CCCCB), and other relevant entities process and analyze data shared within the framework of annual reports, especially in the sectoral view of cybersecurity issues in Slovakia[23]. These form a publicly available and comprehensive document for professionals, the academic sector, and the lay public.

As in other countries of the European Union, the digital space in Slovakia was and remains affected by the war conflict in Ukraine. In connection with the war in Ukraine, the National Centre recorded several attempts at DDoS attacks (distributed denial of service attacks) on web news portals and state institutions in the Slovak cyberspace. The National Centre, therefore, issued recommendations to all portal operators on how to prevent such attacks. Among the recommendations for the operators of news portals are the introduction of monitoring of website operation and the number of inquiries, the optimisation of site performance, and the use of public CDNs (Content Delivery Networks). The National Centre further advised operating web servers in several locations with different Internet connections, using DDoS protection services, blocking attackers carefully, being ready to react, and trying to actively search the web, forums, and social networks for information about planned attacks[24].

The manifestation of general global trends[25] confirmed the fact that the entry vector into the systems is, in most cases, the leakage or acquisition of login data of one of the company's employees (supported by the trend of transition to home office) or the abuse of vulnerabilities of devices or systems freely available through the Internet. Based on experience, ransomware infection still has the most severe consequences for the functioning of both individuals and organisations. The National Security Agency has identified the continued activity of professional gangs providing ransomware as a service in this area. Ransomware is one of the most significant global security threats to governments, businesses, and individuals. In 2023, Slovakia became a new member of the Counter Ransomware Initiative (CRI), which unites countries

23 *A Report on Cybersecurity in the Slovak Republic in 2022*, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/sprava_kyber_2022.pdf [access: 3.02.2024].

24 *They recorded several attempts at cyberattacks on news websites*, https://www.teraz.sk/slovensko/nckb-zaznamenalo-viacero-pokusov-o-utok/615335-clanok.html [access: 3.02.2024].

25 *General global trends* [in:] *A Report on Cybersecurity in the Slovak*...

from all over the world. The CRI consists of several working branches, and Slovakia has joined all of them, such as the International Anti-Ransomware Working Group, the group that focuses on rulemaking, and the group that focuses on diplomacy. The initiative was created in October 2021 as a response to ransomware which has been an increasingly prominent threat with severe economic and security implications. The National Security Office has repeatedly identified, in the Cybersecurity Reports in the Slovak Republic, that this type of illegal activity in the online space has a growing tendency.

Based on the detection of the National Centre for Cybersecurity SK-CERT, mandatory reports from basic service providers and digital service providers, and voluntary reports from Slovak companies, private individuals, partners, and partner organisations, the following incidents were identified in the previous period:

Table 1. The number of detected, reported, and resolved incidents in 2021, by type of incident

Type of incident	Message detected	Solution
Botnet	57 608	67
Unavailability (DoS, DDoS...)	40 681	85
Wrong approach	13	28
Unwanted content	308	308
Fraud	6	22
Penetration attempt	4 107	1 512
Penetration into the system	89	139
Malicious code	7 003	607
Obtaining information	477 349	1 415
Vulnerability	169	121
Other	58 077	142

Source: NCKB SK-CERT[26].

The National Centre notes that the graphic display of statistics does not include incidents or security events in the Unwanted Content category that were detected based on signatures on security elements. There was a total of 48 887 103 of these potential incidents in 2022. Most incidents were detected and reported in May 2022, and most were resolved in December 2022.

26 *The number of detected, reported and resolved incidents for 2021, by type of incident* [in:] *A Report on Cybersecurity in the Slovak...*

Table 2. Cybersecurity incident reports across sectors in 2022

Sector	Number of reports
Banking	131
Transportation	8
Digital infrastructure	7
Electronic communications	14
Energy	6
The post office	32
Industry	8
Public services	328
Healthcare	52
Other	584

Source: NCKB SK-CERT[27].

A significant experience was the NATO Summit in Vilnius in July 2023. It brought the further capability of the North Atlantic Alliance in the field of cybersecurity. During a two-day meeting of NATO representatives, a new system was launched to increase resistance to cyberattacks. This is a new capability of the Alliance to deal with dangerous cyber activities under the name VCISC (Virtual Cyber Incident Support Capability). VCISC represents a system of cyber support that NATO members provide to each other. The system works voluntarily, and members contribute their security infrastructure to it. The VCISC system is overseen by the command of the North Atlantic Alliance, which also acts as an intermediary for information sharing and cyber security coordination. The Allies successfully tested the VCSIC capability for the first time during the NATO summit in Vilnius with a fake cyberattack. During the exam, they tested the safety of communication equipment and coordination. Some participating allies, including Slovakia, joined the VCISC system in Lithuania from abroad to provide the Lithuanian National Cybersecurity Centre with the necessary virtual and technical support during the summit.

A key problem of the past and future is the lack of professionals in the field of cybersecurity. For example, Slovakia currently has only 86 certified auditors, and approximately 52 companies are engaged in cybersecurity auditing. The number of applicants for cybersecurity audits in our certification

27 *Cybersecurity incident reports across sectors in 2022*, in: *A Report on Cybersecurity in the Slovak Republic in 2022*, p. 11, https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/sprava_kyber_2022.pdf [access: 5.02.2024].

Centres is decreasing year-on-year. So far, ten have been successful in 2023. From this, it can be interpreted that interest is dramatically decreasing, and we do not expect this to change soon. The reason for the low number of auditors is mainly the demanding qualification requirements. Even the amendment to the Act on Cybersecurity, after which the cybersecurity audit could affect almost 17,000 Slovak companies, will not probably change the situation. In such a case, 300 to 600 certified auditors would be needed in Slovakia[28].

Slovakia must focus its attention on improving the staffing of experts educated and certified to handle challenges in the field of cybersecurity because, otherwise, we will be forced to bear the consequences.

Conclusion

The protection of cybersecurity has become extremely important due to the numerous cases of attacks, including hacking and data breaches. In order to be effective, such protection requires not only the use of technical security measures such as firewalls or antivirus software but also staff knowing how to counter cyberattacks. In practice, a major disruption of ICT systems can result in social services being unavailable, and even in the paralysis of the state. Lack of access to the network makes it impossible to use financial resources, transport control systems and some medical services and to supervise electricity grids while disrupted electricity supplies trigger further disruptions affecting all elements of critical infrastructure[29].

Given the need to ensure the proper functioning of the state and its tasks in cyberspace, assuring cybersecurity becomes extremely important. The protection of cyberspace must be continuous and apply not only in times of crises or conflicts (although in such circumstances, it is particularly required) but also when the state uninterruptedly performs its tasks. In the latter case,

28 I. Makatura, *Slovakia lacks cybersecurity auditors*, https://www.nbu.gov.sk/2023/11/23/slovensku-chybaju-auditori-kybernetickej-bezpecnosti/index.html [access: 5.02.2024].

29 M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2, p. 646–647. In the age of a state whose operations rely on ICT systems, interference with their functioning can also take place through cyberattacks, M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5, p. 50.

such protection has a preventive character[30]. Failure to provide adequate protection levels can undermine citizens' trust in the public authority. It is expected to take measures to ensure cybersecurity and to enforce the application of proper safeguards by other actors to avoid the paralysis of the public or private sector operations as a consequence of cyberattacks[31].

Cyberthreats can lead to negative phenomena of different sorts and trigger crises. This is particularly true when cyberattacks are aimed at ICT systems, including those related to the continuity of critical infrastructure operations. Cyberthreats can lead to emergencies given that states are highly computerised and their ICT systems are not always adequately protected[32].

With cybersecurity in mind, the adequate level of protection of the ICT systems needs to be ensured. However, it should be stressed that, in some specific instances, this may involve restrictions on the freedoms and rights of an individual in cyberspace[33]. Such restrictions are permissible if the cyberthreat is of an aggravated nature and cannot be countered otherwise.

Bibliography

Adamczyk M., Karpiuk M., Soler U., *The use of new technologies in education – opportunities, risks and challenges in the times of intensive intercultural change*, „Edukacja Międzykulturowa" 2023, no. 4.

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

Bencsik A., Karpiuk M., *The legal status of the cyberarmy in Hungary and Poland. An overview*, „Cybersecurity and Law" 2023, no. 2.

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

Blicharz J., Zacharko L., *Kilka refleksji na temat rozumienia nowoczesnej administracji publicznej*, „Gubernaculum et Administratio" 2022, no. 1.

Chałubińska-Jentkiewicz K., *Cyberodpowiedzialność*, Toruń 2019.

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, „Studia Iuridica Lublinensia" 2021, no. 4.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, „Studia Iuridica Lublinensia" 2023, no. 5.

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

31 M. Karpiuk, A. Makuch, U. Soler, *The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity*, „Polish Political Science Yearbook" 2023, no. 3, p. 156.

32 M. Karpiuk, *Crisis management vs. cyberthreats*, „Sicurezza, Terrorismo e Societa" 2022, no. 2, p. 114.

33 M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, „Studia Iuridica Lublinensia" 2022, no. 3, p. 34.

Czuryk M., *Cybersecurity as a premise to introduce a state of exception*, „Cybersecurity and Law" 2021, no. 2.
Czuryk M., *Special rules of remuneration for individuals performing cybersecurity tasks*, „Cybersecurity and Law" 2022, 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., *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.
Gawkowski K., *Cyberbezpieczeństwo w inteligentnym mieście*, „Cybersecurity and Law" 2023, no. 2.
Hoffmam 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., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki 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., *Computer fraud*, „Cybersecurity and Law" 2023, no. 2.
Karpiuk M. , *Crisis management vs. cyberthreats*, „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., *Tasks of the Minister of National Defense 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.
Karpiuk M., Kelemen M., *Cybersecurity in civil aviation in Poland and Slovakia*, „Cybersecurity and Law" 2022, no. 2.
Karpiuk M., Makuch A., Soler U., *The role of the Cybersecurity Strategy of the Republic of Poland in ensuring cybersecurity*, „Polish Political Science Yearbook" 2023, no. 3.
Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, „Prawo i Więź" 2023, no. 4.
Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, 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.
Kuś B. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. K. Chałubińska-Jentkiewicz, M. Karpiuk, J. Kostrubiec, Warszawa 2022.
Nowikowska M., [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.
Pieczywok A., *Cyberspace as a source of dehumanization 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.
Prokopowicz D., Matosek M., *Importance and Security of Information Provided by the Internet in the Context of the Development of Economic Entities in Poland*, „International Journal of New Economics and Social Sciences" 2017, no. 2.
Raport roczny z działalności CERT Polska 2022. Krajobraz polskiego Internetu, Warszawa 2023.
Romaniuk P., *Kształtowanie administracyjnoprawnych warunków służących do budowy cyberbezpieczeństwa w administracji publicznej*, „Cybersecurity and Law" 2023, no. 2.

Romaniuk P., *Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną*, „Studia Prawnoustrojowe" 2022, no. 58.
Szpor G. [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. G. Szpor, A. Gryszczyńska, K. Czaplicki, Warszawa 2019.
Tyrawa D., *Krajowy system cyberbezpieczeństwa w świetle nauki prawa administracyjnego. Uwagi wybrane*, „International Journal of Legal Studies" 2023, no. 1.
Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1.

Zagrożenia cyberbezpieczeństwa w Ukrainie, Polsce i na Słowacji

Streszczenie

Problematyka poruszana w artykule dotyczy cyberzagrożeń występujących w Ukrainie, Polsce oraz na Słowacji. Systemy teleinformatyczne w państwie cyfrowym odgrywają ważną rolę, dlatego na państwie ciąży obowiązek należytej ich ochrony. Ingerencja w normalne funkcjonowanie takich systemów może mieć daleko idące konsekwencje, nawet prowadzić do paraliżu określonych sektorów gospodarczych. Konieczność ciągłego monitoringu zjawisk występujących w cyberprzestrzeni wynika ze stałej obecności w niej cyberzagrożeń, ich intensywności i rodzaju. Pozwala to na przeciwdziałanie cyberatakom i tym samym unikanie ich negatywnych skutków. Autorzy wskazują m.in. typy incydentów oraz ich liczby.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenia