Ius et Securitas 2/2025 | ISSN 3071-799X

Valentin Constantinov
Moldova State University
ORCID: 0000-0001-9578-1134
walentkonstant@yahoo.fr

Mirosław Karpiuk
University of Warmia and Mazury in Olsztyn
ORCID: 0000-0001-7012-8999
miroslaw.karpiuk@uwm.edu.pl

Nicola Strizzolo
University of Teramo
ORCID: 0000-0001-6384-9210
nstrizzolo@unite.it

Cybersecurity Incidents as Threats to National and International Security

Abstract

In connection with the development of an information society, which is not only a matter of individual states but has been increasingly discussed from an international perspective, cybersecurity must be seen as an international issue. Such a perception of cybersecurity is also determined by the fact that, given the development of an information society, the state must keep pace with its evolving needs and evolve in the digital sphere. The increasing use of cyberspace for various activities triggers new threats, which take the form of cybersecurity incidents. Cyberattacks occur in all countries using ICT systems. As one could hardly imagine living without access to the Internet, a global network, we are all vulnerable to cyberattacks.

This article aims to present cybersecurity not only as a national domain but also as an international one, as cyberattacks are faced not by one or several countries but by all countries globally. The article also attempts to outline the most frequent types of incidents and the serious threats they entail. The primary research method employed in the article was the case study. Analytic and synthetic methods were also used.

Keywords: cyberthreats, cyberspace, cybersecurity.

Introduction

Cybersecurity is not a domain that can be considered only from a national perspective, as it has an international dimension. Security-compromising phenomena are increasingly encountered in cyberspace, which has a cross-border nature and cannot be confined within national borders. Some cybersecurity incidents also occur at a cross-border level. As a result, attempts to combat them cannot be made using the means and resources available to one state, as they will prove ineffective and will not eliminate the problem at its source. Instead, they will essentially focus on mitigating the effects of a cyber threat rather than eliminating the threat itself.

Serious threats to the functioning of public institutions or business entities can also emerge in individual countries, with cyberattacks paralysing the operation of their strategic sectors. Such attacks are often aimed against critical infrastructure which is expected to protect important branches of the economy or areas of the state's activities. However, the effects of such cyberattacks can be seen (whether directly or indirectly) in other countries as well.

The international dimension of cybersecurity does not merely imply that incidents can bring consequences for several countries and that access to cyberspace is generally unlimited. It also means that cyberattacks occur in every country because of the widespread use of ICT systems in virtually any area of human life.

Information and communication technologies have become the foundation for economic development. Given the use of these technologies by key service operators, digital service providers and critical infrastructure operators, they constitute critical elements in ensuring the security of citizens and the continuity of the state's operations. For this reason, ensuring cybersecurity must be treated as a priority.[1]

Due to technological progress and digitisation of public and private lives, states must protect their citizens and institutions against cyber threats whose consequences can be very severe, including the destabilisation of public authorities. Digitisation is only feasible with the universal use of ICT systems. However, as these systems are susceptible to disruptions, both the state and

[1] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Warsaw 2017, p. 12.

private entities must use their best endeavours to minimise these disruptions which, in some cases, may significantly reduce the possibilities to perform tasks, provide services and exchange communication[2].

Digital transformation cannot be limited to establishing infrastructure and updating software, nor can it reflect a range of random decisions and ongoing political fights. Instead, a clear and coherent digital strategy is needed, covering areas such as the state, cybersecurity, skills and the economy. Successful digitisation is conditional upon such elements as security, trust, efficiency and universal access. The use of the digital space should, therefore, be secure[3].

The purpose of this article is to analyse cybersecurity as a supranational phenomenon. It contains examples of incidents that have occurred in individual states, exerting a significant influence on certain sectors of their activities.

Cybersecurity incidents

According to the EU legislator, "incident" means an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services offered by, or accessible via, network and information systems. A category of large-scale cybersecurity incidents has also been established, covering incidents causing a level of disruption that exceeds a Member State's capacity to respond to it or which significantly impacts at least two Member States[4].

Each EU Member State was required to establish at least one Computer Security Incident Response Team (CSIRT). Pursuant to Article 11(3) of the NIS 2 Directive, CSIRT teams perform the following tasks: 1) monitoring and analysing cyberthreats, vulnerabilities and incidents at the national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and

[2] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, p. 1.

[3] K. Gawkowski, D. Standerski, *Cyfrowe państwo. Strategia dla Polski*, Warsaw 2023, p. 25.

[4] Article 6 (6)-(7) of Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive 2) (OJ EU L 333, p. 80-152).

information systems; 2) providing early warnings, alerts, announcements and dissemination of information to essential and important entities concerned as well as to the competent authorities and other relevant stakeholders on cyberthreats, vulnerabilities and incidents, if possible in near real-time; 3) responding to incidents and providing assistance to the essential and important entities concerned, where applicable; 4) collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity; 5) providing, upon request from an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact; 6) participating in the CSIRTs network and providing mutual assistance in accordance with their capacities and competencies to other members of the CSIRTs network upon their request; 7) acting as a coordinator for the purposes of the coordinated vulnerability disclosure; and 8) contributing to the deployment of secure information-sharing tools.

The Polish legislator indicates the following tasks assigned to CSIRTs: 1) monitoring cybersecurity threats and incidents at the national level; 2) estimating risks related to the identified cybersecurity threats and incidents, along with conducting dynamic risk analysis; 3) providing information on incidents and risks to the national cybersecurity system entities; 4) releasing notifications of the identified cybersecurity threats; and 5) responding to reported incidents[5]. At the same time, CSIRTs must fulfil the relevant requirements necessary to guarantee effective and compatible incident and risk handling capabilities, and to ensure cooperation at the EU level. They are expected to contribute to developing trust and confidence between EU Member States and promote and develop rapid and effective operational cooperation[6].

As in the previous years, phishing was the most common incident type recorded in 2023 by CERT Polska (acting as CSIRT NASK[7]), with 41423

[5] Article 26 (3) of the National Cybersecurity System Act of 5 July 2018 (consolidated text, Journal of Laws of 2024, item 1077, as amended), hereinafter: the NCSA. See also Z. Nowak, *Agencja Cyberbezpieczeństwa – polska wersja The National Cybersecurity Centre, Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, K. Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik [eds.], Gliwice 2024, p. 169.

[6] M. Nowikowska, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz [eds.], Warsaw 2019, p. 197.

[7] CSIRT NASK is the Computer Security Incident Response Team operating at the na-

incidents, accounting for as many as 51.61% of all incidents handled in 2023. This number increased by more than half compared to the previous year. Actions exploiting the image of Allegro (a Polish online e-commerce platform) were the most common – 11161 cases, followed by those exploiting the image of Facebook – 5308 cases, and OLX (a Polish sales site) – 4753 cases. Another common type of incident was computer fraud, with 34304 cases, accounting for more than 42% of all incidents recorded in 2023. These included fake online shops and financial fraud involving the unlawful use of the images of various types of oil and energy companies, businesses and institutions. Malware was the third most common incident type (in terms of the number of incidents recorded). A total of 1650 incidents of this type were recorded, half as many as in the previous year. These ranged from ransomware use to spam campaigns distributing Remcos and Agent Tesla software. In 2023, 40 incidents were handled that were classified as serious, including 31 in the banking sector and 9 in the healthcare sector[8]. Pursuant to Article 2(7) of the NCSA, a serious incident is an incident which causes or is likely to cause a serious deterioration in the quality or interruption of the continuity of a key service.

In 2023, CSIRT GOV[9] in Poland, within the area of its competence, received a total of 322656 reports of potential cybersecurity incidents, 43785 of which were eventually classified as actual cybersecurity incidents. There was a significant increase in the number of incidents in the social engineering category. Incidents of this type were mainly related to social engineering campaigns using email. Among these, phishing and spear-phishing attacks were identified. These were aimed at illegally obtaining login details, soliciting payments or phishing for other sensitive data. Attempts to launch malware attacks were also reported. In 2023, CSIRT GOV received 11 incident

tional level, run by the Research and Academic Computer Network – the National Research Institute. For more details on the qualities of CSIRT NASK, see also M. Karpiuk, *The obligations of public entities within the national cybersecurity system*, „Cybersecurity and Law" 2020, No. 2; J. Kostrubiec, *The position of the Computer Security Incidents Response Teams in the national cybersecurity system*, „Cybersecurity and Law" 2022, No. 2; M. Karpiuk, *Competence of the CSIRT NASK Team in the Field of Combating Abuse of Electronic Communications*, „Cybersecurity and Law" 2024, No. 2.

[8] *Raport roczny z działalności CERT Polska 2023*, Warsaw 2024, pp. 102-103.

[9] CSIRT GOV is the Computer Security Incident Response Team operating at the national level, run by the Head of the Internal Security Agency.

reports considered serious. All incidents of this type were merely malfunctions and they did not indicate activities meant as cyberattacks[10].

In the 2000s, incidents like the Blaster worm that hit an Ohio nuclear plant or the attacks on Brazil's power grid demonstrated how vulnerable these infrastructures were[11]. Although security systems have improved, recent events such as the Colonial Pipeline attack (2021) [12] and intrusions into Ukraine's energy systems (2015-2016)[13] show that the risks not only persist but have evolved, becoming more sophisticated and harder to prevent.

The scenarios for hacker attacks can include: 1) widespread blackouts: between 2015 and 2016, cyberattacks in Ukraine left thousands of citizens without electricity[14], in June 2003, a nuclear power plant in Ohio was compromised by a worm, causing a five-hour failure in the plant's safety monitoring system[15], in 2005 and 2008, hackers infiltrated the control systems of Brazil's power grid[16], in January 2008, power outages in five unnamed U.S. cities were caused by cyberattacks[17]; 2) interruptions of essential services, the 2021 Colonial Pipeline attacks paralyzed fuel distribution in the U.S., causing panic and economic losses exceeding $4 million[18].

The 2024 presidential elections in Romania deeply shook Romanian society from the end of that year and into the first months of the following year, 2025. After the first round of voting, unexpectedly and despite all prior opinion polls, an unknown candidate, Călin Georgescu, who ran as an independent, came in first place. In second place was Elena Lasconi, the mayor of the municipality of Câmpulung (Câmpulung Muscel, Argeș County), who had since become the president of the Save Romania Union (USR) party.

---

[10] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023*, Warsaw 2024, p. 8, 12.

[11] N. Strizzolo, *Smart grid, i pericoli di una rete energetica connessa*, https://www.agendadigitale.eu/sicurezza/smart-grid-i-pericoli-di-una-rete-energetica-connessa/, [accessed: 22.01.2025].

[12] *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, https://www.cisa.gov/, [accessed: 18.11.2024].

[13] R.M. Lee, M.J. Assante, T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington 2016.

[14] Ibidem.

[15] N. Strizzolo, *Smart grid, i pericoli di una rete energetica connessa*, https://www.agendadigitale.eu/sicurezza/smart-grid-i-pericoli-di-una-rete-energetica-connessa/, [accessed: 23.01.2024].

[16] Ibidem.

[17] Ibidem.

[18] *DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, https://www.cisa.gov, [accessed: 18.11.2024].

Thus, the main candidate expected to make it to the second round, Marcel Ciolacu from the Social Democratic Party (PSD), did not qualify. The ranking was as follows: Călin Georgescu 22.94%; Elena Lasconi 19.18%; and Marcel Ciolacu 19.15%. The difference was minimal – only 2,740 votes – yet Marcel Ciolacu found himself out of the presidential race[19].

Later, former President Traian Băsescu stated that the annulment of the elections was made at the intervention of PSD officials, omitting to mention that the decision was actually taken by the Constitutional Court after an intervention by the incumbent president Klaus Iohannis, who was not affiliated with PSD[20].

It must be said that many aspects of the 2024 Romanian presidential affair will likely remain unknown or at least classified as Top Secret. Therefore, our analysis can only be based on deduction. First of all, Romanian society may have shown naivety by prematurely dismissing the possibility of a „foreign factor" being involved and interested in the affair. From the first statements, analysts, experts, and reporters excluded the Russian factor from the equation, which contributed to the strengthening of the position of the aforementioned candidate who led in the first round. The situation was even more curious considering that Russian cyber involvement had played major roles in much more powerful and technologically advanced states such as the USA or Germany. This was the first mistake made by the establishment. It meant that such influential forces had to be „found" within the country itself. Of course, aside from some populist statements blaming one institution or another, nothing concrete was established. Again, valuable time was lost, during which Georgescu's „populist" positions became even more firmly established, the country became divided in two, and Georgescu's supporters kept repeating the same message – it is a democratic right to vote for whomever we choose[21].

---

[19] *Pentru alegerea Președintelui României*, https://prezidentiale2024.bec.ro/rezultate-turul-i-2/, [accessed: 11.05.2024].

[20] *Traian Băsescu îl acuză pe Marcel Ciolacu că a „recurs la anularea alegerilor" pentru că a ratat intrarea în turul 2 / Ce spune despre „furtul de la Paris"*, https://hotnews.ro/traian-basescu-il-acuza-pe-marcel-ciolacu-ca-a-recurs-la-anularea-alegerilor-pentru-ca-a-ratat-intrarea-in-turul-2-ce-spune-despre-furtul-de-la-paris-1957290, [accessed: 11.05.2024].

[21] *Cine este Călin Georgescu. Un portret în zece puncte: unde a lucrat, cu cine, de când vrea să fie președinte și cine îl susține*, https://romania.europalibera.org/a/cine-este-calin-georgescu/33322895.html, [accessed: 13.05.2024].

Only two days before the second round of voting, the Constitutional Court annulled the first round and announced the organization of new elections. The official statement revealed that, based on received intelligence, a massive foreign intervention had been identified which had tilted the elections in favor of „one of the candidates". This marked an unprecedented event in Romania's post-Communist history (since the fall of the Ceaușescu regime).

Now, the Constitutional Court of Romania (CCR) made this decision following the declassification of documents presented during a meeting of the Supreme Council of National Defense (CSAT), which indicated that the electoral process had been „compromised throughout its entire duration". The documents revealed a campaign of „Russian hybrid attacks" aimed at favoring the independent candidate Călin Georgescu[22].

Additional details were added regarding what served as the basis for the annulment of the elections. Among the identified irregularities were: 1) the illegal use of digital technologies, including artificial intelligence, during the campaign; 2) undeclared financing of Georgescu's campaign, estimated at up to 1 million euros, despite official statements claiming „zero lei"; 3) cyberattacks on Romania's electoral systems, attributed to Russia. The CCR concluded that these elements had compromised the integrity of the elections, necessitating the restart of the entire electoral process.

The arguments presented by the Constitutional Court were not accepted by the media nor by several categories of citizens. The two frontrunners from the first round, Călin Georgescu and Elena Lasconi, were the first to oppose the decision. Subsequently, polls were conducted to determine which of the two candidates Romanians would choose as president in the second round. According to these results, Călin Georgescu would have won by a significant margin. It is likely that Romanian society is still not ready to accept a woman at the head of the state.

The presidential elections in Romania were particularly telling in the territory of the Republic of Moldova, where over 50% of the population also holds Romanian citizenship. Romania organized 59 polling stations in the Republic of Moldova, where over 80,000 voters participated. This represents a notable increase in the number of voters among Moldovan citizens. For example, in

[22] *Privind anularea procesului electoral cu privire la alegerea Președintelui*, https://www.ccr.ro/wp-content/uploads/2024/12/Hotarare_32_2024.pdf, [accessed: 13.05.2024].

the second round of the 2009 elections, Traian Băsescu received 94.62% of the votes from Moldovan voters, but from only about 12,000 participants. Therefore, in about ten years, the number of voters in Moldova for the Romanian presidential elections has increased by approximately 6.67 times[23].

What is more important is this: if, in 2009, the votes of Moldovans proved decisive for Traian Băsescu, in the first round of 2024, those same Moldovans overwhelmingly supported Elena Lasconi, who received 45,590 votes, corresponding to 56.65% of the total votes cast there. Notably, the „leader" of the first round, Călin Georgescu, received just over 2,500 votes in the presidential elections in Moldova, representing approximately 3.11% of the total votes cast by Romanian citizens in Moldova.

The second aspect we want to draw attention to: From this point forward, the Republic of Moldova will play an important role in all types of elections in Romania, especially considering the 2,740-vote difference by which Elena Lasconi surpassed the acting Prime Minister Marcel Ciolacu. This element is also considered very significant by those who believe that the involvement of social media networks in Romania was orchestrated by internal forces. Former Romanian President Traian Băsescu believes that if Marcel Ciolacu had made it to the second round, the elections would not have been annulled. This is why this turn of events is so important. With the votes from abroad, Elena Lasconi managed another turnaround and secured second place, which guaranteed her a spot in the final.

Călin Georgescu's message fits into the „sovereigntist" category – anti-NATO, anti-EU – and he has repeatedly expressed sympathy for Russia. This fact could serve, at least for those who are not very familiar with the election details, as an argument for the cyber involvement of Russian Federation intelligence services in Romania's 2024 elections.

It is clear that someone was deeply involved in Romania's 2024 presidential campaign. The motives and intentions vary from case to case. Unfortunately, the public only has one official statement: that "foreign forces", specifically Russian, were involved in these elections. Let us recall that a large part of the Romanian political class refuses to acknowledge this idea. Let's take it step by step.

[23] *Prezență record la alegerile românești în R. Moldova*, https://moldova.europalibera.org/a/romanii-isi-aleg-presedintele-cum-decurge-procesul-de-votare-in-r-moldova/33213856.html, [accessed: 14.05.2024].

Undoubtedly, the situation surrounding Romania's presidential elections shows that the relevant institutions and cyber intelligence services were not prepared to counter such an attack. The second issue is that Romanian legislation is not aligned with this kind of threat. And since the state institutions were overwhelmed by the situation, the simplest solution is to remain silent – to avoid declaring that a cyberattack favored one candidate, leading to the annulment of the elections and their removal from the presidential race for allegedly benefiting from such interference. In fact, it was not hard to determine that, a few days before the first round, on social media – particularly TikTok, but also Facebook – several fake accounts appeared promoting aggressive pro-Călin Georgescu propaganda. The messages promoted in these posts were the same ones the candidate used during the campaign: the country is in danger, it has been sold to foreigners, and it must be reclaimed for Romanians; externally, good relations with Russia must be restored, especially since both Russians and Romanians are Orthodox Christians.

However, a large part of the electorate claims they were not influenced by TikTok or Facebook. They say they consciously wanted to vote against a political class that has long since degraded and no longer meets the necessary standards. Moreover, they argue that the current class is far inferior to the "nomenklatura" that occupied the political stage immediately after the December 1989 Revolution. That is why they believe they have the right to continue voting for Călin Georgescu, the anti-system candidate, in a system that is hopelessly corrupt. According to them, eliminating Călin Georgescu amounted to a coup d'état, and the "mafia-like liberal-social democrat nomenklatura" defeated the people's will for a renewal of Romania's heavily degraded political class.

In recent times, Romania has been governed by a coalition of its two most important political parties: the Social Democratic Party (PSD) and the National Liberal Party (PNL), which traces its origins to Ion Iliescu, the first president of Romania after 1989, who was accused of taking over the former communist nomenklatura. Interestingly, despite the accusations against it, the PSD remains at the forefront of Romanian political life.

The PNL claims to be the descendant of the historic party founded in the second half of the 19th century by the Brătianu family and revived after the 1989 Revolution. It has positioned itself in opposition to the PSD as a right-wing party. However, for quite some time now, especially during periods of

crisis, and at the suggestion of Romanian business leaders, several national unity governments have been formed, involving both major parties along with other smaller ones.

It is difficult to pronounce a definitive judgment on the expectations of the Romanian electorate. One idea would be to consider the evolution of Romania's GDP over the last 10 years, a period during which, according to the electorate, the political class has significantly deteriorated. Yet, between 2015 and 2024, Romania's GDP almost doubled, increasing from USD 178 billion to over USD 384 billion. It is worth noting that in the pandemic year of 2020, the economy contracted by 3.7%. Some analyses forecast growth in the next 10 years to as much as 700 billion euros. In terms of GDP per capita adjusted for purchasing power parity, Romania has reached 80% of the European Union average, surpassing seven other European countries. Additionally, as of 2025, Romania has been accepted into the Schengen Area. Despite this, the Romanian electorate remains dissatisfied with the country and desires a political class different from that of the past 10 years[24].

Nevertheless, regardless of how the presidential elections turn out, we believe this example will serve as a lesson not only for Romanian decision-makers – who will take appropriate measures to prevent cyber interference in support of one candidate or another – but also for many other European countries and their political classes, who, by observing the Romanian case, may be able to prevent similar disruptions in their own nations.

Conclusions

Social and economic development is increasingly dependent on the rapid and unhindered access to, as well as the use of, information in management, production, and the service and public sectors. The dynamic development of information systems fosters the development of the economy, particularly in communication, trade, transport and financial services. The digital technologies which make up cyberspace contribute to shaping social relations, and services provided via the Internet have become tools for influencing so-

[24] *ZF 26 de ani. PIB şi creştere economică. De unde am plecat, unde am ajuns?*, https://www.zf.ro/banci-si-asigurari/zf-26-de-ani-pib-si-crestere-economica-de-unde-am-plecat-unde-am-22560715, [accessed: 15.05.2024].

cial groups' behaviour and means of exerting political influence. Any significant disruption in the functioning of cyberspace, whether of a global or local nature, is likely to affect the security of business transactions, the sense of security among citizens, the operational efficiency of public sector institutions, production and service processes, and – in consequence – overall national security[25].

Taking into consideration the specific nature of entities operating in cyberspace, individual states and European and international institutions must support efforts to prevent cybersecurity incidents. They need to establish appropriate legal regulations to eliminate cyber threats and run campaigns to draw attention to the consequences of cyberattacks, promote the desirable social attitudes related to the responsible use of the Internet, and support actions to increase digital competencies.

Confidence in digital services can only be built on a strong security foundation. As cybercrime is not confined within borders, it is important to be constantly prepared to face new forms of potential online security breaches. Cybersecurity should be a constant element in the digital space from first contact with the Internet – through school, professional and private lives[26]. Cybersecurity education helps reduce the risk of cyberattacks and thus provides the appropriate protection level for the ICT systems used not only for private purposes but also for public, business or social activities. Cyber hygiene, as a derivative element of cybersecurity knowledge, enables avoiding cybersecurity incidents or mitigating their effects and ensures sufficient privacy protection on the Internet.

Bibliography

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

Gawkowski K., Standerski D., *Cyfrowe państwo. Strategia dla Polski*, Warsaw 2023.

Karpiuk M., *Competence of the CSIRT NASK Team in the Field of Combating Abuse of Electronic Communications*, "Cybersecurity and Law" 2024, No. 2.

[25] The Cybersecurity Strategy of the Republic of Poland for 2019-2024, appended to Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Strategy of the Republic of Poland for 2019-2024 (Official Gazette of the Government of the Republic of Poland of 2019, item 1037), p. 5.

[26] K. Gawkowski, D. Standerski, *Cyfrowe*..., pp. 29-30.

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

Kostrubiec J., *The position of the Computer Security Incidents Response Teams in the national cybersecurity system*, "Cybersecurity and Law" 2022, No. 2.

Lee R.M., Assante M.J., Conway T., *Analysis of the Cyber Attack on the Ukrainian Power Grid*, Washington 2016.

Nowak Z., *Agencja Cyberbezpieczeństwa – polska wersja The National Cybersecurity Centre, Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii*, [in:] *Bezpieczeństwo narodowe Rzeczypospolitej Polskiej. 25 lat członkostwa w NATO*, K. Chałubińska-Jentkiewicz, K. Gawkowski, Z. Nowak, Ł. Piątkowski, K. Wąsik [eds.], Gliwice 2024.

Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz [eds.], Warsaw 2019.

* * *

Incydenty cyberbezpieczeństwa jako zagrożenia o charakterze krajowym i międzynarodowym

Streszczenie

W związku z rozwojem społeczeństwa informacyjnego, które nie jest tylko domeną pojedynczych państw, a coraz częściej ujmowane jest w kategoriach międzynarodowych, cyberbezpieczeństwo należy postrzegać jako instytucję międzynarodową. Takie postrzeganie cyberbezpieczeństwa determinuje również fakt, że w związku z rozwojem takiego społeczeństwa państwo musi nadążać za jego potrzebami i tym samym rozwijać się cyfrowo. Wraz z coraz częstszym wykorzystywaniem do różnej aktywności cyberprzestrzeni pojawiają się nowe zagrożenia, które przybierają postać incydentów cyberbezpieczeństwa. Cyberataki występują w każdym państwie, które korzysta z systemów teleinformatycznych. Trudno sobie dzisiaj wyobrazić życia bez Internetu będącego siecią globalną, a jeżeli korzystamy z niego to jesteśmy narażeni na cyberataki.

Celem artykułu jest zwrócenie uwagi na cyberbezpieczeństwo nie tylko jako domenę krajową, ale również międzynarodową, dlatego, że z cyberatakami mamy do czynienia nie w jednym, czy w kilku państwach, ale na całym świecie. Celem jest również przykładowe wskazanie jakie incydenty występują najczęściej oraz jakie wywołują poważne zagrożenia. Podstawową metodą badawczą wykorzystaną w pracy było studium przypadku. Zastosowano również analizę, jak też syntezę.

Słowa kluczowe: cyberzagrożenia, cyberprzestrzeń, cyberbezpieczeństwo.