Świat Idei i Polityki • 2024, t. 23, nr 2, s. 75–88
World of Ideas and Politics • 2024, vol. 23, no. 2, pp. 75–88
ISSN 1643-8442
DOI: 10.34767/SIIP.2024.02.05

Andrzej Pieczywok[1]

Institutional and legal dimensions in state cybersecurity policy

SUMMARY This article aims to identify the key institutional and legal dimensions of state cybersecurity policy, which are increasingly shaped by the growing use of digital resources. The central research question is: What are the most distinctive institutional and legal dimensions in state cybersecurity policy? The main hypothesis posits that these dimensions are primarily defined by specific EU strategies and directives, as well as legal regulations related to the Civil Code. Cybercrime threats, including viruses, malware, online fraud, and phishing, significantly influence these dimensions, as users of digital resources are often targeted by such attacks. The publication used several research methods, including analysis of source documents and subject literature as well as the institutional and legal methods.

KEYWORDS threats, security, legislation, cyber responsibility policy, education, digital resources

Introduction

At the turn of the 21st century, the significance of new media surged, revolutionizing human communication processes. Social media platforms have become integral to modern life, making the ability to navigate communication and information technologies a crucial skill acquired through education. This heightened interest in new technologies reflects their growing economic role. Rapid information flow determines success, and the knowledge stored in information databases is vital for decision-making processes (Bratland, Siemieniecka & Siemieniecki,

[1] Andrzej Pieczywok Prof. Dr. hab., Faculty of Political Science and Administration, Department of Security Policy, Kazimierz Wielki University in Bydgoszcz, e-mail: a.pieczywok@wp.pl, ORCID: 0000-0002-4531-0630.

2016). Access to this knowledge depends on the ability to utilize information tools such as Wikipedia and integrated information management systems. New media have evolved from mere intermediaries in information transmission to active participants in communication. They have become essential tools for intellectual support, and interactions with new media lead to the phenomenon of the "extended mind." The internet is now not only a repository of information but also a platform for the development and dissemination of culture, art, ideas, philosophical views, and above all, knowledge (Siemieniecka & Siemieniecki, 2019, p. 12).

Digitization is transforming the world across all aspects and fields of life. The omnipresence of modern technologies and media in everyday life is undeniable. Many activities that were traditionally carried out just a few years ago are now unimaginable in any form other than digital. Most of society now lives in a world of digital content and services, permeating daily life to an unprecedented extent. However, what fosters innovation in everyday life can also pose significant threats which are often underestimated.

Ensuring cybersecurity and creating a unified digital market for the future has become a top priority for every state. Given the complexity of cybersecurity issues and the diversity of involved entities, states must continually reassess their cybersecurity models, taking into account the international security environment, interpreted as a strategic security context encompassing political, economic, and military dimensions.

Cybersecurity, extensively studied by various researchers for years, remains an area of particular interest, including by European Union institutions and bodies. The multifaceted nature of cybersecurity issues means that this topic is increasingly considered not only in terms of protecting key systems and networks but also from the perspective of state policy regarding the use of digital resources. Researchers are increasingly convinced that contemporary learning cannot exist in isolation from technology and new media, particularly information and communication technologies (Salehi, Shojaee & Sattar, 2015, p. 64; Klichowski, 2017, pp. 27–28), multimedia, and social media.

Conversely, the virtual world exposes us to increasing dangers. Defending against these threats is not an easy task. Current Polish regulations do not provide for criminal liability for acts of cyberbullying. This means there is no provision in criminal law that specifically addresses cyberbullying. However, this does not imply complete impunity for perpetrators. Cyberbullying infringes

on personal rights, such as dignity and reputation. When cyberbullying actions cause personal harm, civil legal action can be pursued.

Key concepts related to the legal dimensions of using digital resources

Responsibility, in its broadest sense, is defined as the "willingness to bear the consequences of one's choices, decisions, and behaviors" (Nowicka-Kozioł, 2000, p. 8). It also involves consciously and voluntarily undertaking commitments to perform one's duties to the best of one's ability, including tasks that benefit others.

Responsibility thus encompasses a wide range of meanings. It can imply not only accountability for performing actions but also for their consequences and being ready to face sanctions for non-performance or improper performance. There is no area of collective life, human coexistence, or human behavior to which the ambiguous term "responsibility" does not apply. It is used in various contexts and meanings, such as moral and legal responsibility; professional and parental responsibility; bearing and imposing responsibility; responsibility for something and to someone; responsible people and responsible work; and the conditions and manifestations of responsibility (Michalik, 1998, p. 20).

Defining the concept of cyber-responsibility first requires addressing what "legal responsibility" means. Although this term is fundamental in the legal system, it lacks a uniform definition. The primary issue in defining this term relates to the meaning of "responsibility," which varies depending on the context. For example, we speak of moral, political, and social responsibility.

Previous considerations allow for defining cyberspace in various ways. Notably, the concept of an information society is of particular interest. The term information society originated in Japan, first used by Tadao Umesao (1963) in his article on the theory of the evolution of a society based on information technologies. It was later popularized by Kenichi Koyama (1968) in his dissertation *Introduction to Information Theory* (Globan-Klas & Sienkiewicz, 1999, p. 42).

The term "information society" describes a community at a high level of technological development, where information is the most valuable and commonly exchanged asset (Golka, 2008). This information is intensively used in economic, social, cultural, and political life, treated as a special intangible resource, often more valuable than material goods. This society possesses rich means of communication and information processing, forming the basis for generating most

national income and providing livelihood for most people (Szewczyk, 2007). For its participants, computers, the internet, and all digital technologies become one of the most important aspects of life and work.

Another crucial issue is information security. It ensures the confidentiality, integrity, availability, and authenticity of information, eliminating threats such as unauthorized disclosure, modification, or destruction of information by unrecognized entities.

The concept of network and information security was defined in Regulation (EC) No. 460/2004 of the European Parliament and Council of 10 March 2004, establishing the European Network and Information Security Agency as "the ability of a network or information system to withstand, with a given level of confidence, any action that compromises the availability, authenticity, integrity, and confidentiality of stored or transmitted data and the services accessible via those networks and systems."

Another term related to digital resources is cyberspace. Cyberspace is a complex environment resulting from the interaction of people, software, and services on the internet through technical devices and connected networks, which does not exist physically. Gradually, the term cyberspace has been used by scholars to identify phenomena not created by human imagination, describing virtual connections (Aleksandrowicz & Liedel, 2014, p. 23).

Some authors define cyberspace as a network of interdependent IT infrastructure, including the internet, telecommunications networks, computer systems, embedded processors, and controllers in strategically important industrial environments, as well as copper cables, internet routers, fiber optics, relay towers, and satellite transponders (Katzan, 2012, p. 72).

This understanding of cyberspace indicates that it is directly embedded in the physical space through the entire teleinformatics infrastructure. Such definitions are usually used to describe "state cyberspaces."

Pierre Lévy, a French sociologist and author of the concept of cyberculture, defines cyberspace as "a new space enabling communication, social interactions, organization, and transactions" (Lévy, 2004). Lévy also emphasizes the emergence of a new market for information and knowledge, resulting from contemporary technical evolution. Cyberspace is studied by sociologists, with references to this discipline found in some national cybersecurity strategies.

In another view, the term cyberspace is used to describe virtual connections arising and functioning through their physical manifestations – computers and

telecommunications infrastructure. In this interpretation, cyberspace is often considered synonymous with the internet.

One of the most known and widely cited definitions of cyberspace was formulated by the U.S. Department of Defense in an attempt to create a unified dictionary of military and associated terminology. According to this definition, cyberspace is the global domain of the information environment, consisting of interdependent networks created by IT infrastructure and stored data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers (Wasilewski, 2013, p. 227). Various definitions have also been proposed in Polish literature. According to Ryszard Tadeusiewicz, "cyberspace encompasses all hardware and software tools related to the techniques of collecting, processing, transmitting, and sharing information, used by people to acquire knowledge and communicate with others" (Tadeusiewicz, 2010, p. 32). This definition emphasizes that the internet is currently the most important, though not the only, component of cyberspace. This dual-aspect definition is noted by Jakub Rzucidło and Justyna Węgrzyn (2015, p. 152), highlighting cyberspace as both technical infrastructure and a realm of human interactions involving this infrastructure. These interactions often lead to cyber threats.

Cyber threats that can impact cybersecurity are diverse and dynamic. Many types of cyber threats exist, but their catalog is not closed as new threats continuously emerge. Various classifications can be found in the literature due to different definitions, criteria, and the pace of change.

Both cyberspace and cyber threats relate to the knowledge area of cybersecurity. Cybersecurity involves protecting computer systems from malicious attacks or espionage. It encompasses all techniques and tools used to protect infrastructure and the confidentiality, integrity, and availability of data stored or exchanged in the digital world.

The definition of cybersecurity includes all actions – methods, procedures, and legal solutions – undertaken by relevant entities to ensure the integrity of collected, stored, and processed information resources, protecting them from unauthorized disclosure, alteration, or destruction. However, this definition may seem limited to information protection, not addressing many other threats that may not be directly related to any illegal use of information but could involve criminal activities using IT tools or information itself. Such situations may involve the trafficking of prohibited goods, child pornography, or fraud (Chałubińska-Jentkiewicz, 2019, p. 23–24).

As stated in the Cybersecurity Policy (Ministry of Administration and Digitization, 2013, p. 5), cybersecurity is "a set of organizational, legal, technical, physical, and educational measures aimed at ensuring the uninterrupted functioning of cyberspace." It relates to both civil and military tasks to counter physical threats to systems (cyberspace security) and virtual threats to users (security in cyberspace). Alongside cyberspace and cybersecurity, terms such as cyberattack (deliberate disruption of cyberspace functioning), cyber threats (technological information threats), cybercrime, cyberterrorism, cyber espionage, and cyber warfare have become more popular. These terms, both in Poland and globally, are characterized by significant conceptual divergence and frequent lack of precision (Bączek, 2011, p. 73).

In legal regulations, lawmakers have attempted to define criminal acts involving information and systems that process this information and establish the scope of liability for illegal actions. However, alongside information security, the concept of cybersecurity has emerged, defined as all actions – methods, procedures, and legal solutions – undertaken by relevant entities to ensure the integrity of collected, stored, and processed information resources, protecting them from unauthorized disclosure, alteration, or destruction (Potejko, 2009, p. 194).

The European Union's response to cybersecurity regulation challenges

In recent years, the European Union has seen a significant increase in incidents that threaten the functioning of networks and information systems. The EU responded to these threats with Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for a high common level of security of network and information systems across the Union, known as the NIS Directive (Albrycht et al., 2019, p. 45).

In 2017, as part of a review of the EU Cybersecurity Strategy, actions were initiated to establish the "EU Cybersecurity Package," which encompasses a comprehensive set of measures focused on three key areas: resilience, prevention, and defense.

In December 2020, the European Commission and the European External Action Service (EEAS) introduced a new EU cybersecurity strategy aimed at enhancing Europe's resilience to cyber threats and ensuring all citizens and businesses have access to trustworthy digital tools and services. This strategy includes specific proposals for regulatory, investment, and policy instruments.

It addresses the security of essential services such as hospitals, energy grids, and railways, as well as the growing number of connected devices in homes, offices, and factories.

On 22 March 2021, the Council adopted conclusions on the cybersecurity strategy, emphasizing that cybersecurity is crucial for building a resilient, green, and digital Europe. The primary goal set by EU ministers was to ensure strategic autonomy while maintaining an open economy. This involves enhancing the capacity for independent decision-making in cybersecurity to strengthen the EU's digital leadership and strategic capabilities.

The EU's commitment to cybersecurity regulation is undeniable. This is evidenced not only by the analysis of debates within and between EU institutions and member states but also by research on EU legislation. To bolster its resilience to future challenges, the EU seeks to improve cross-sectoral and cross-border crisis management, enhance crisis communication, and intensify the fight against disinformation. Key areas in EU crisis management tools and regulations include the civil protection mechanism, integrated political crisis response, health emergency preparedness and response, protection of networks and information systems, and critical infrastructure protection.

In May 2023, the Council approved conclusions on cyber defense, stressing that the EU and its member states must further strengthen their resilience to cybersecurity threats and enhance collective cybersecurity and cyber defense against harmful behaviors and acts of aggression in cyberspace.

An example of implementing the NIS Directive is Poland's Act of 5 July 2018 on the National Cybersecurity System. This Act establishes three national-level Computer Security Incident Response Teams (CSIRTs):

1. CSIRT GOV, operated by the Head of the Internal Security Agency;
2. CSIRT MON, operated by the Minister of National Defense;
3. CSIRT NASK, operated by the Research and Academic Computer Network – National Research Institute.

The Polish National Cybersecurity Policy Framework for 2017–2022 continues the government's efforts to enhance cybersecurity in Poland, building on the 2013 Cybersecurity Protection Policy of the Republic of Poland. Both national development strategies and those related to public order and national security depend on the implementation of IT systems.

This document aims to outline framework actions to achieve a high level of resilience in national IT systems, key service operators, critical infrastructure

operators, digital service providers, and public administration against incidents in cyberspace.

The Civil Code's provisions, according to the classification of responsibility by fault, risk, and equity, include the following regulations:

- Responsibility based on fault: Article 416 – liability of legal persons; Article 417; Article 429 – fault in selection.
- Responsibility based on risk: Article 430 – damage caused by a subordinate; Article 433 – throwing, spilling, falling; Article 434 – collapse of a building; Article 435 – liability of the operator of an enterprise or plant; Article 436 – liability of the possessor of a mechanical means of transport.
- Responsibility based on equity: Article 417 – liability for damage caused by public authority; Article 428 – liability in the absence of obligated supervisors; Article 431 – damage caused by animals (Chałubińska-Jentkiewicz, 2019, p. 108).

Currently, over 50 legal acts related to new technology law are being developed in Poland and the EU. Below is a list of the most important of these legal acts, divided into specific thematic areas of new technologies (cybersecurity, e-privacy, e-commerce, innovation, the internet, telecommunications, intellectual property, and data management).

Effective cybersecurity is a priority not only at the national level but also among allies. Frequent attacks on government and military servers in many countries, the cyber war between Russia and Ukraine, and threats from North Korea's leader to crucial American institutions and the economy highlight the emergence of a new battlefield in a previously unknown domain.

Beyond the institutional-legal approach, a crucial area of security policy involves fostering proper civic awareness. This can be achieved through education at various social levels: schoolchildren, adults, and seniors. Cyber threats constantly evolve, making cybersecurity education a continually changing and sometimes challenging field.

Cybersecurity education is vital for equipping future employees with the awareness, skills, and knowledge necessary to adapt and diversify in this field. The EU's new initiative aims to raise cybersecurity awareness among workers and citizens, regardless of their current professional activity. Even retirees or older adults need cybersecurity knowledge and awareness when using digital services through connected devices.

Learning through engaging puzzles and educational games significantly impacts students' cybersecurity outcomes. The goal is to help students acquire

knowledge at their own pace about various cybersecurity challenges and enable them to develop ethical hacking skills in a much safer environment.

The role of information and communication technologies in state education policy

Information and communication technologies (ICT) play a crucial role in shaping the institutional and legal dimensions of state cybersecurity policy, especially within the education sector. The emergence of digital space is a result of the development of modern digital resources, including advanced technologies and media. Early attempts to integrate ICT into education began in the early 20th century.

Over the past two decades, the application of ICT in education has significantly expanded, leading to the creation of new technology-enhanced learning (TEL) models such as e-learning, m-learning, and u-learning, ultimately culminating in the sophisticated concept of smart education (Bielinis, 2022, p. 29).

Categorizing ICT is challenging and depends on specific criteria, such as interaction solutions or types of software. A good starting point is the concepts of Web 2.0 and social media. These terms emerged simultaneously, making their distinction difficult without a broader perspective. The term Web 2.0 first appeared in 1999 in an article by Darcy DiNucci, who described the then-static internet as the "embryo" of what was to come (DiNucci, 1999, pp. 220–222). Web 2.0 involves users co-creating content on internet platforms, rather than being passive recipients.

Andreas Kaplan and Michael Haenlein (2018) define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content" (Kaplan & Haenlein, 2018). Thus, the Web 2.0 philosophy has driven the creation of social media platforms, applications, and the blogosphere.

Today, communication increasingly takes place in the digital space via social media, which integrates human community activities and practices on the internet and facilitates dialogue. The language used online is a unique form of communication that allows simultaneous interaction through text, sound, and graphics. Children and adolescents use emoticons, acronyms, and other verbal-visual forms, creating various language variations online (Tanaś, 2015, pp. 12–13). The first and second decades of the 21st century saw the emergence of numerous social media platforms, messaging apps, and internet tools such as Facebook,

Twitter, GoldenLine, LinkedIn, YouTube, Instagram, Snapchat, ResearchGate, and Academia.edu (including the now-defunct Edmodo and Nasza Klasa, transformed into nk.pl).

Wikipedia is one of the most popular internet tools due to its widespread use and active user involvement in content creation. Blogs, another key tool, are types of websites with chronologically ordered entries, allowing for archiving, categorizing, tagging, and reader comments.

The sheer number of tools available for educational purposes is vast. As the internet evolves, so does the terminology, with the concept of Web 3.0 emerging shortly after Web 2.0. The virtual world provides an environment where various characters, elements, situations, or behavior patterns can be created and used for diverse purposes, from virtual social gatherings to educational activities.

Distance learning design is supported by various IT systems, including:

- Learning Management Systems (LMS),
- Learning Content Management Systems (LCMS),
- Learning Communication Systems (LCS).

E-learning platforms are among the most popular educational tools in universities, schools, and organizations, significantly supporting educational activities and enabling systematic management of educational content.

Authoring tools are a category of software designed for creating and editing e-learning course content. These tools include those for developing course elements like text, graphics, animation, sound, and video, and for assembling these elements into a coherent course. Customizing courses with institutional logos and templates enhances their appeal and serves as a marketing tool for the institution.

Careful selection of activities and tools, along with proper course component integration, directly impacts the quality and effectiveness of the course, leading to greater participant satisfaction.

Mobile innovations are increasingly integrated into daily life, with mobile connectivity allowing for the management of both personal and professional activities. The number of mobile device users is growing worldwide and in Poland.

Mobile devices continue to evolve, with expanding functionalities such as photo editing, text formatting, video and audio recording, navigation, calendars, and multimedia playback. Their development suggests they may reach critical mass due to continuously added features, such as GPS (Hojnacki, 2013, pp. 114–115).

The capabilities of mobile technologies allow them to be considered educational tools. Mobile apps provide continuous access to training content and other educational resources, including podcasts, videos, and e-books. An intuitive content layout facilitates efficient information acquisition, test completion, and progress tracking.

In security education, mobile device functionalities such as GPS can be used in field exercises to locate students and expedite task completion. The use of such features in teaching depends on the instructor's creativity.

The potential of mobile devices makes them increasingly promising tools for teachers. However, their use and the development of training content for these devices require continuous improvement and familiarity with new approaches. This challenge is accompanied by curiosity about how such support will perform in classrooms or other educational settings.

Augmented reality (AR) enhances the real world by adding virtual elements, which can be used for various purposes, particularly education. Advanced AR technologies enable users to interact in virtual environments, communicate with others (human or AI), and engage in immersive experiences.

Devices used in virtual reality (VR) environments, besides head-mounted displays (HMDs), include:

- Motion tracking devices (without displays) such as inertial, magnetic, ultrasonic, and optical trackers;
- Sensor gloves that track finger movements and hand gestures, and measure pressure on buttons;
- 3D navigation controllers (joysticks, mice) and shooting game guns;
- Stereoscopic displays: monitors, boards, walls, projectors;
- Haptic feedback devices like vibrating chairs, moving seats, interactive vests, and grippers that interact with the user's body (hands, back, head), and VR-equipped workstations (Brzostek-Pawłowska, 2009, p. 31).

Conclusions

The analyses confirm that the initial hypothesis, as stated in the abstract, has been partially validated. The institutional and legal dimensions of state cybersecurity policy are indeed shaped by specific EU strategies and directives, as well as legal regulations within the Civil Code. Additionally, various threats associated with cybercrime and the responsibilities tied to the use of modern information and communication technologies significantly impact these dimensions.

Moreover, the implementation of institutional and legal frameworks is influenced by ongoing innovations in information technologies, which continually set new trends for ensuring and developing cybersecurity measures. As technology evolves, national legal standards must be progressively aligned with international regulations, particularly EU laws, to effectively combat cybercrime and ensure robust cybersecurity.

The primary objective of cyber-responsibility policy is to ensure cybersecurity, a responsibility that rests on all network users. Public administration bodies play a crucial role in this process, with one of their fundamental tasks being to maintain safety and public order.

Current legal regulations regarding cyberspace and cybercrime only partially meet the regulatory requirements. The assessment of legal frameworks related to cyber-responsibility policy reveals significant gaps that necessitate the development of new approaches.

While most legal regulations concerning information are justified, they are insufficient. For instance, the right to privacy should be protected not only during crises but also in everyday life. In the Polish legal system, there are no specialized regulations specifically addressing cybercrimes; they are instead prosecuted under general laws and provisions related to various situations involving computers or telecommunication networks.

Cyberspace presents a genuine risk of surveillance by both criminals and security agencies responsible for protecting the state's critical interests and maintaining public order. The boundary between ensuring security and infringing on individual rights and freedoms is very narrow. Network users are sensitive to attempts to monitor their activities while simultaneously demanding security, which the state, as the responsible public authority, is expected to provide.

References

Albrycht, I. et al. (2019). *Wyzwania w cyberprzestrzeni. Przykłady rozwiązań, zagrożenia, regulacje.* Kraków: Wydawnictwo Instytutu Kościuszki.

Aleksandrowicz, R & Liedel, K. (2014). Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia. In: K. Liedel, P. Piasecka & T.R. Aleksandrowicz (eds.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji.* Warszawa: Wydawnictwo Difin.

Bączek, P. (2011). *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego.* Toruń: Wydawnictwo Adam Marszałek.

Bielinis, L. (2022). *Uczenie się w przestrzeniach cyfrowych uniwersytetu studium teoretyczno-empiryczne*. Kraków: Oficyna Wydawnicza Impuls.

Bratland, E., Siemieniecka, D. & Siemieniecki, B. (2016). *Knowledge, ICT and Education: A Variety of Perspectives*. Toruń: Wydawnictwo Adam Marszałek.

Brzostek-Pawłowska, J. (2013). E-learning, wirtualny i realny świat. *Prace Naukowo-Badawcze Instytutu Maszyn Matematycznych*, 2, 31.

Chałubińska-Jentkiewicz, K. (2019). *Cyberodpowiedzialność.* Toruń: Wydawnictwo Adam Marszałek.

DiNucci, D. (1999). Fragmented future. *Print*, *53*(4), 220–222. Retrieved from: http://darcyd.com/fragmented_future.pdf [accessed: 20.10.2023].

Globan-Klas, T. & Sienkiewicz, P. (1999). *Wprowadzenie do teorii informacji.* Kraków: Wydawnictwo Fundacja Postępu Technicznego.

Golka, M. (2008). *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*. Warszawa: Wydawnictwo Naukowe PWN.

Hojnacki, L. (ed.) (2013). *Mobilna edukacja. (r)ewolucja w nauczaniu – poradnik dla edukatorów*. Think!. Wirtualna Biblioteka Nowoczesnego Nauczyciela i Ucznia, Epub, 114-115.

Kaplan, A.M. & Haenlein, M. (2018). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1). DOI: https://doi.org/10.1016/j.bushor.2009.09.003

Katzan, H. (2012). Cybersecurity Service Model. *Journal of Service Science* 2, 72. DOI: https://doi.org.10.19030/jss.v5i2.7576

Klichowski, M. (2017). *Learning in CyberParks. A theoretical and empirical study.* Poznań: Wydawnictwo Uniwersytetu im. Adama Mickiewicza.

Lévy, P. (27.11.2004). *Drugi potop*. Retrieved from: http://portal.tezeusz.pl/cms/tz/index.php?id=287 [accessed: 20.02.2022].

Michalik, M. (1998). O niektórych paradoksach odpowiedzialności. In: A.M. de Tchorzewski (ed.), *Odpowiedzialność jako wartość i problem edukacyjny*, *Odpowiedzialność jako wartość i problem edukacyjny.* Bydgoszcz: Wydawnictwo „Wers".

Nowicka-Kozioł, M. (2000). *Wprowadzenie. Poczucie odpowiedzialności moralnej jako aspekt podmiotowy.* Warszawa: Wydawnictwo Akademickie „Żak".

Potejko, P. (2009). Bezpieczeństwo informacyjne. In: K.A. Wojtaszczyk, A. Materska-Sosnowska (eds.), *Bezpieczeństwo państwa*. Warszawa: Wydawnictwo ASPRA JR.

Rozporządzenie 460/2004 (2004). *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 460/2004 z dnia 10 marca 2004 r. ustanawiające Europejską Agencję do spraw Bezpieczeństwa Sieci i Informacji.* Dz. Urz. UE L 2004 nr 77.

Rzucidło, J. & Węgrzyn, J. (2015). Stany nadzwyczajne w sytuacji szczególnego zagrożenia państwa w cyberprzestrzeni. *Przegląd Prawa Konstytucyjnego*, 5, 142. DOI: https://doi.org.10.15804/ppk.2015.05.07

Salehi, H., Shojaee, M. & Sattar, S. (2015). Using e-Learning and ICT Courses in educational environment, A Review. *English Language Teaching*, 8, 63–70. DOI: https://doi.org.10.5539/elt.v8n1p63

Siemieniecka, D. & Siemieniecki, B. (2019). *Teorie kształcenia w świecie cyfrowym.* Kraków: Oficyna Wydawnicza Impuls.

Szewczyk, A. (2007). Społeczeństwo informacyjne – nowa jakość życia społecznego. In: eadem (ed.), *Społeczeństwo informacyjne – problemy rozwoju.* Warszawa: Wydawnictwo Difin.

Tadeusiewicz, T. (2010). Zagrożenia w cyberprzestrzeni. *Nauka*, 4, 32.

Tanaś, M. (2015). Prolegomena do pedagogiki medialnej. In: M. Tanaś & S. Galanciak (eds.), *Cyberprzestrzeń, człowiek, edukacja:* Vol. 1. *Cyfrowa przestrzeń kształcenia* (pp. 7–25). Kraków: Oficyna Wydawnicza Impuls.

Uchwała Rady Ministrów z 25 czerwca 2013 r. Ministerstwo Administracji i Cyfryzacji przy współpracy z Agencji Bezpieczeństwa Wewnętrznego.

Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, 9, 227.

Wymiary instytucjonalno-prawne w polityce cyberbezpieczeństwa państwa

STRESZCZENIE Celem artykułu jest identyfikacja najważniejszych wymiarów instytucjonalno-prawnych w polityce cyberbezpieczeństwa państwa. Wymiary te spowodowane są zwiększonym korzystaniem z zasobów cyfrowych. Sformułowany główny problem badawczy brzmi następująco: jakie wymiary instytucjonalno-prawne są najbardziej charakterystyczne w polityce cyberbezpieczeństwa państwa? Przyjęto następująco hipotezę główną: przypuszcza się, że najbardziej charakterystycznymi wymiarami instytucjonalno-prawnymi w polityce cyberbezpieczeństwa państwa są określone strategie i dyrektywy Unii Europejskiej, a także regulacje prawne związane z Kodeksem cywilnym. Decydujący wpływ na obecność tych wymiarów mają zagrożenia związane z cyberprzestępczością, gdyż to właśnie użytkownicy zasobów cyfrowych są głównie ofiarami wirusów i innego szkodliwego oprogramowania, oszustw internetowych oraz *phishingu* (wyłudzenia poufnych informacji). W publikacji wykorzystano kilka metod badawczych, były to: analiza dokumentów źródłowych i literatury przedmiotu oraz metoda instytucjonalno-prawna.

SŁOWA KLUCZOWE zagrożenia, bezpieczeństwo, ustawodawstwo, polityka cyberodpowiedzialności, edukacja, zasoby cyfrowe

Date of submission of the article: 21.02.2024; date of acceptance of the article: 3.07.2024.