Articles

Studia Iuridica Lublinensia vol. 34, 1, 2025
DOI: 10.17951/sil.2025.34.1.73-95

Christophe Gaie
French Prime Minister Services, France
ORCID: 0000-0002-8252-5278
christophe.gaie@gmail.com

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

Andrea Spaziani
University of Teramo, Italy
ORCID: 0000-0002-2465-3570
aspaziani@unite.it

Cybersecurity in France, Poland and Italy

Cyberbezpieczeństwo we Francji, Polsce i Włoszech

ABSTRACT

Presently, cyberspace dominates private lives and is extensively used for business activities, including providing services and implementing public tasks. It facilitates conducting various activities, both public and non-public, reducing costs as well as increasing accessibility. Cyberspace also enables faster communication. Therefore, its importance can hardly be overestimated. However, with the development of new technologies and the widespread use of the Internet, cyberthreats are

CORRESPONDENCE ADDRESS: Christophe Gaie, PhD, French Prime Minister Services, Engineering and Innovation Department, Paris 07, France; Mirosław Karpiuk, PhD, Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, Obitza 1, 10-725 Olsztyn, Poland; Andrea Spaziani, PhD Student, University of Teramo, Department of Political Science, R. Balzarini 1, 64100 Teramo, Italy.

intensifying. Measures to combat them should be vital parts of any entrepreneur's or web user's activities, and public policies at the central, local and regional levels. Through adequate cybersecurity management using cyberspace can be optimised and the threats it poses countered.

Keywords: cybersecurity; cyberspace; computer fraud; malware

INTRODUCTION

While cyberspace is, in a sense, an abstract notion for humans, it has a tangible impact on the reality in which both societies and states operate. The specific location of network services does not, in any way, determine where data is processed. Cyber-attacks can be carried out from anywhere globally, against any target.[1]

In cyberspace, we deal with increasingly blurred boundaries and a limited ability to supervise activities pursued there. This makes some users believe they are anonymous, which may prompt them to engage in illegal or quasi-legal activities. Cyberspace is also where criminals or services of hostile states are active. Therefore, it must be properly protected against such negative phenomena.

The protection of cyberspace against threats rests, i.a., with administrative bodies which sometimes need to resort to measures posing considerable nuisance to combat threats.[2] Such measures must effectively prevent threats that significantly reduce the resilience of commonly used ICT systems and threats that affect the proper functioning of the state and its institutions. In this regard, it is essential to manage cybersecurity in a way that not only eliminates the effects of such threats but also anticipates and prevents them. Given the specificity of the digital society and state, and the current importance of e-communication and information, which is processed by various actors and to various extents, security in cyberspace must be properly protected to avoid significant disruptions.[3]

The issues of cybersecurity, and its administrative and legal aspects, have been dealt with by several authors, including M. Czuryk, J. Kostrubiec, A. Bencsik and, in the context of media law, by K. Chałubińska-Jentkiewicz. Research into cybercrime has been conducted, i.a., by F. Radoniewicz.

To determine the status of cybersecurity research, the literature on the subject was analysed. The normative aspects of the protection of cyberspace against threats were determined using the doctrinal legal-research method. The article aims to identify threats existing in cyberspace, along with solutions to prevent and combat them.

---

[1] K. Kaczmarek, *Vulnerability to Cyber Threats: A Qualitative Analysis from Societal and Institutional Perspectives*, "Cybersecurity and Law" 2024, no. 2, pp. 107–108.

[2] K. Kaczmarek, M. Karpiuk, C. Melchior, *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3, p. 125.

[3] M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4, pp. 8–9.

CYBERSECURITY IN FRANCE

The contemporary world faces a rapidly escalating threat of cyberattacks. These attacks, growing exponentially, target critical infrastructure, steal sensitive data and disrupt essential services. To safeguard their fundamental interests, nations must prioritize robust cybersecurity strategies.[4]

France's focus on cybersecurity can be traced back to the early 2000s, when the country undertook the process of protecting against the growing threat of cyberattacks. In 2008, the White Paper on Defence and National Security identified cyber threats as a major challenge and called for the development of a national cybersecurity strategy.[5] This White Paper was supported by the President of the French Republic, Nicolas Sarkozy.

Then, in 2009, the French government established the National Information Systems Security Agency (ANSSI) to oversee cybersecurity policy and operations. The ANSSI has played a central role in developing and implementing France's cybersecurity strategy, which has focused on protecting critical infrastructure, preventing and investigating cybercrimes, raising awareness and education of citizens and companies and promoting innovation and research.[6]

At the beginning of 2010, the French government decided to implement a strategy to make France a leader in the field of cybersecurity. A concrete measure to strengthen the country was to extend the ANSSI's range of action to critical infrastructures and operators such as network and energy companies.[7]

France's 2015 national cybersecurity strategy,[8] designed to support the digital shift and address evolving threats, has been expanded to make cybersecurity a competitive edge for French businesses. This was followed by a strategic review of cyber defence published by the Secrétariat général de la défense nationale (SGDSN) in February 2018 as an important part of the national defence strategy. This was outlined by the French War Minister, Florence Parly, who considers cyber is a weapon, with a potential that can be far more harmful and dangerous than a missile.[9]

---

[4] H. Luiijf, K. Besseling, M. Spoelstra, P. Graaf, *Ten National Cyber Security Strategies: A Comparison*, [in:] *Critical Information Infrastructure Security*, eds. S. Bologna, B. Hämmerli, D. Gritzalis, S. Wolthusen, Cham 2013.

[5] *The French White Paper on Defence and National Security*, 9.7.2008, https://www.europarl.europa.eu/cmsdata/175477/20080711ATT34025EN.pdf (access: 10.6.2024).

[6] *What We Do*, https://cyber.gouv.fr/en/what-we-do (access: 10.5.2024).

[7] *The French Critical Infrastructures Information Protection (CIIP) Framework*, https://cyber.gouv.fr/en/french-ciip-framework (access: 10.5.2024).

[8] Stratégie nationale pour la sécurité du numérique, https://cyber.gouv.fr/sites/default/files/document/strategie_nationale_securite_numerique_fr.pdf (access: 10.5.2024).

[9] A speech given by Florence Parly, French Minister of Armies, in Lille on 8 September 2021.

France also made significant investments to accelerate progress in the field of cybersecurity with the "Plan Cyber" that is part of the national strategy "France 2030", in which the government allocated EUR 1 billion over five years to the domain from 2021 to 2025.[10] This strategy sets ambitious goals: tripling the cybersecurity industry's turnover to EUR 25 billion by 2025, doubling the number of jobs to 75,000, and nurturing the creation of three French cybersecurity unicorns.

To ensure the protection of a nation's economic and strategic interests, several key dimensions must be considered (see Figure 1). This section details these dimensions and explains how France achieves its objectives in each area.

Figure 1. Illustration of the dimensions of cybersecurity in France

Source: own elaboration.

Critical infrastructure protection. This focuses on safeguarding essential systems like energy grids, transportation networks and financial institutions from cyberattacks. France prioritizes securing these critical infrastructures to ensure national security and prevent widespread disruption. France has defined 12 sectors of vital importance and assigned them to a minister in charge of leading their cyberprotection.

[10] *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, 2021, https://www.info.gouv.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite (access: 18.5.2024).

Table 1. List of the 12 French sectors of vital importance

Sector of vital importance		Coordinating minister
1	Civilian Activities of the State	Minister of the Interior
2	Judicial Activities	Minister of Justice
3	State Military Activities	Minister of Defense
4	Food	Minister of Agriculture
5	Electronic Communications, Audiovisual, Information	Minister of Electronic Communications
6	Energy	Minister of Energy
7	Space and Research	Minister of Research
8	Finance	Minister of Economy and Finance
9	Water Management	Minister of Ecology
10	Industry	Minister of Industry
11	Health	Minister of Health
12	Transportation	Minister of Transportation

Source: own elaboration.

Cybercrime prevention and investigation. This dimension involves working actively to combat cybercrime through law enforcement collaboration. French authorities work to identify, investigate and prosecute cybercriminals, aiming to deter future attacks and bring perpetrators to justice. France adopted complementary doctrines for defensive, offensive and influence cyber operations to face cyber threats (data theft, sabotage, paralysis of institutions, etc.) that concern both civil and military domains: 1) Defensive Information Operations (DIO) is the set of actions implemented to protect information systems against cyberattacks. It aims to anticipate, detect, and respond to threats in order to preserve the confidentiality, integrity, and availability of data and systems; 2) Offensive Information Operations (OIW) is the set of actions implemented to attack an adversary's information systems. It aims to collect information, disrupt the operation of systems, or cause damage; 3) Information Influence Operations (IIO) is a multifaceted tactic that manipulates public opinion or individual behavior through information systems, or identifies such manipulations. The offensive approach encompasses a range of techniques, including spreading disinformation or propaganda to sow discord, demoralizing or dividing a population to undermine trust in institutions, disrupting democratic processes to hinder fair elections, and inciting social unrest to destabilize societies.

It is important to understand that organizing cybersecurity defence is complex, with elements related to national defence being directed by the President of the Republic as Head of the Armed Forces, and on the other hand, the Prime Minister steering the action of all ministries. Figure 2 is inspired by the scheme proposed by Le Guédard.[11]

[11] *Organisation de l'État français en gestion de crise cybernétique majeure*, https://www.ihemi.fr/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure (access: 18.5.2024).

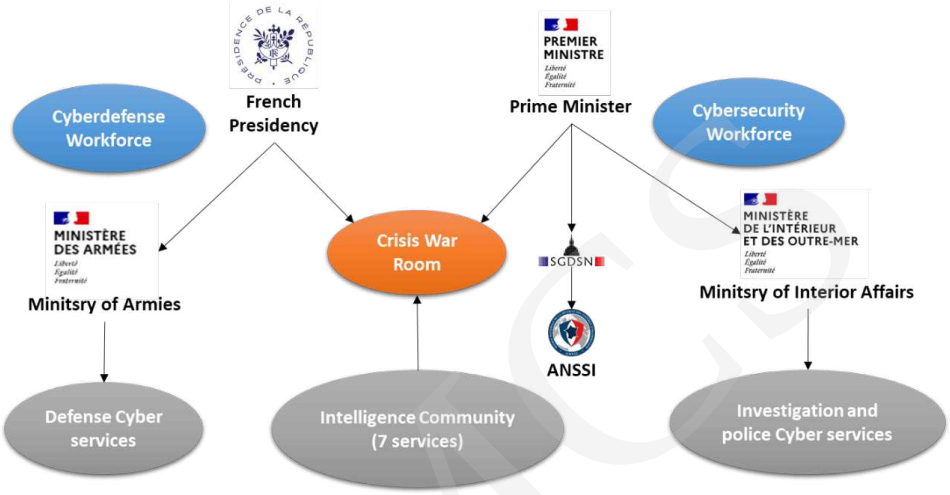

Figure 2. Simplified organization of cybersecurity in France

Source: own elaboration.

Public and business awareness and education. Educating the public and businesses about cybersecurity risks and best practices is crucial. France implements initiatives to raise awareness about potential threats, phishing scams and how individuals and organizations can protect themselves online.

The ANSSI recognizes the critical need for cybersecurity education and awareness among all citizens. To address this growing concern, the agency has implemented a multifaceted strategy encompassing training initiatives, educational resources and collaborative efforts.[12]

CyberEdu is a program that aims to integrate cybersecurity fundamentals into all non-specialized IT training programs in France. The program is designed to provide students with the knowledge and skills they need to protect themselves and their organizations from cyberattacks.

SecNumedu is a label that is awarded to higher education programs that meet specific cybersecurity criteria. The criteria are designed to ensure that graduates of SecNumedu-labeled programs have the skills and knowledge they need to succeed in the cybersecurity workforce.

[12] *Former et sensibiliser à la sécurité du numérique : un enjeu stratégique pour l'ANSSI*, https://cyber.gouv.fr/actualites/former-et-sensibiliser-la-securite-du-numerique-un-enjeu-strategique-pour-lanssi (access: 28.5.2024).

Initiated by the ANSSI, CyberEdu and SecNumedu programs foster a thriving cybersecurity ecosystem in France.[13] These programs empower students with the necessary skills to excel in cybersecurity careers, providing employers with a wellspring of qualified professionals. Educational institutions benefit as well, strengthening their program reputation and attracting a new wave of tech-savvy students seeking cybersecurity expertise.

These measures meet one of the strategic objectives defined by the French President of the Republic of "promoting a sustainable defence mindset in society and the state" such as described in the National Strategic Review of 2022.[14]

Innovation and research. France actively supports the development of new cybersecurity technologies and solutions. This involves funding research in cryptography, intrusion detection systems and other areas to stay ahead of evolving cyber threats.

French government services are seeking to play a pioneering role in the innovation and research for robust cybersecurity solutions. This commitment goes beyond simply staying ahead of cyber threats. Initiatives like SPARTA, an EU-backed network aimed at improving research, innovation and training in cybersecurity across Europe,[15] demonstrate France's active role in promoting collaborative research. As a matter of fact, this facilitates the collaboration between government services (ANSSI, CEA), academics (IMT, Inria), companies (Thales) and citizens (YesWeHack).

Specific areas of focus include funding research in cutting-edge cryptography like post-quantum cryptography, a collaboration highlighted by Thales Group,[16] which will be crucial for securing future communications. Additionally, French government websites highlight projects launched under their National Cybersecurity Strategy 2030, which likely involve research into intrusion detection systems and other vital areas.[17] This multi-faceted approach ensures France not only stays

[13] *La formation initiale en cybersécurité*, https://cyber.gouv.fr/formation-initiale-en-cybersecurite (access: 28.5.2024).

[14] *National Strategic Review 2022*, https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf (access: 28.5.2024).

[15] SPARTA, *Re-Imagining the Way Cybersecurity Research, Innovation, and Training Are Performed in the European Union*, 26.2.20219, https://cyber.gouv.fr/sites/default/files/2019/02/communique-de-presse-sparta.pdf (access: 28.5.2024).

[16] *Post-Quantum Cryptography: Six French Cyber Players Join Forces to Design the Secure Communication Networks of Tomorrow*, 15.3.2024, https://www.thalesgroup.com/en/worldwide/security/press_release/post-quantum-cryptography-six-french-cyber-players-join-forces (access: 28.5.2024).

[17] *Presentation of the National Cyber-Strategy: 7 Projects Selected as Part of the Research Priority Readiness Program*, 21.6.2022, https://www.cnrs.fr/en/press/presentation-national-cyber-strategy-7-projects-selected-part-research-priority-readiness (access: 28.5.2024).

abreast of current threats but also actively shapes the future landscape of cybersecurity through cutting-edge research and development.

Moreover, there are numerous initiatives from civil servants to integrate security from the very beginning of an IT project. This can be the case for Human Resources,[18] tax recovery[19] or any other e-government applications. In addition, innovations also focus on cybersecurity mechanisms that can be strengthened through mimicry mechanisms. For instance, it is possible to improve the resilience of the information system by using mechanisms inspired by epidemiology.[20]

International cooperation. Cybersecurity challenges transcend national borders. France actively collaborates with international partners to share best practices, exchange information about threats and coordinate efforts to combat global cybercrime.

The current situation of cybercrime is very challenging for public and private actors who have to struggle against worldwide threats with limited means to defend. Indeed, the interconnected nature of the world renders national borders meaningless in the face of these digital assaults. This pledges for deeper cooperation between established institution that should coordinate deterrence policies and share more information together.[21]

However, the path to effective international collaboration is long and difficult. Indeed, the ideologies of countries are often very different and aim either to limit the information shared concerning their citizens, guarantee the confidentiality of exchanges or maintain tight control over communication. These differences make it difficult to define agreements on how to cooperate against cybercrime.[22]

It was also outlined that the cybersecurity community faces a lack of trust and complex legal issues that hinder the crucial exchange of information.[23] Indeed, Computer Security Incident Response Teams (CSIRTs), also known as Computer Emergency Response Team (CERT), have various compositions (public, private or academics) and consequently follow different objectives (protection of vital interests, business development, research). The national public CERTs are detailed in Table 2.

---

[18] C. Gaie, *Enhancing the Efficiency and the Security of E-Government: The French Case Study of Human Resources Applications*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024.

[19] C. Gaie, M. Mueck, *A Hybrid Blockchain Proposal to Improve Value-Added Tax Recovery*, "International Journal of Internet Technology and Secured Transactions" 2021, vol. 12(1).

[20] J. Langlois-Berthelot, C. Gaie, J. Lebraty, *Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government*, [in:] *Transforming Public Services…*

[21] *Cybersecurity: International Cooperation Requires Reciprocity*, 11.7.2019, https://www.banque-france.fr/en/publications-and-statistics/publications/cybersecurity-international-cooperation-requires-reciprocity (access: 28.5.2024).

[22] R. Hill, *Dealing with Cyber Security Threats: International Cooperation*, Tallinn 2015, pp. 119–134.

[23] S. Bradshaw, *Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*, London 2015.

Table 2. List of the national CERTs in France

	CERT identification	Domain
1	CERT-FR	Interministerial
2	CERT-ANS	Healthcare
3	CERT-PJ	Criminal Investigation Police
4	CERT-RENATER	Education and Research

Source: own elaboration.

The Cybercrime Atlas initiative exemplifies an international platform designed to be a repository of knowledge about the cybercriminal ecosystem.[24] By leveraging shared information from various sources, including government alerts, private sector insights, and even publicly available materials, the Atlas aims to paint a comprehensive picture of this criminal landscape.

This collaborative approach, with its emphasis on information sharing and knowledge exchange, can create a more unified front against cybercrime. Initiatives like the Cybercrime Atlas offer a glimpse into the future, where shared information empowers us to disrupt criminal activities and gain a deeper understanding of the ever-shifting cyber threat landscape.

Legal and regulatory framework. A robust legal framework is essential for addressing cybercrime and data protection. France has established laws and regulations governing data privacy, cybercrime prosecution, and the responsibilities of organizations in protecting user data.

The successive French governments pay a huge attention to ensure data privacy and establish laws to fight against cybercrime. This commitment was initiated by Law No. 78-17 of 6 January 1978 that established the rules to protect data of French citizens.[25] This law defined various aspects of data handling by organizations. A key component is the emphasis on transparency and consent. Organizations must have a clear and legitimate reason for collecting personal data and must obtain unambiguous user consent before processing it. Individuals retain control over their data, possessing the right to access, rectify, or erase it upon request. This provision ensures that individuals are always aware of and in control of how their personal information is used.

The law was later supplemented by the European Union's General Data Protection Regulation (GDPR) that extended the national requirements to every in-

[24] M. Daniel, *How Global Information Sharing Can Help Stop Cybercrime*, 8.6.2023, https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime (access: 4.6.2024).

[25] French Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (Data Protection Act), https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624 (access: 4.6.2024).

formation concerning European citizens in France.[26] The combination of these two regulations is defined as the Data Protection Act (DPA). The law also defines the rules to be followed in terms of data security, incident reporting, and accountability.

As a matter of fact, the law compels organizations to implement appropriate technical and organizational safeguards to protect personal data against unauthorized access, disclosure, alteration or destruction. This requirement compels organizations to continuously assess and enhance their security measures to mitigate potential risks. In case of a data breach, organizations have to notify the relevant authorities to mitigate the impact of cyberattacks.

In terms of organization, data protection and privacy are ensured by the French independent authority – Commission Nationale de l'Informatique et des Libertés (CNIL). This authority plays a major role in enforcing data protection regulations, providing guidance for organizations and handling complaints lodged by individuals concerning their data privacy rights.

CYBERSECURITY IN POLAND

The Polish legislator defines cybersecurity as the ability of information systems to resist any action compromising the confidentiality, integrity, availability and authenticity of processed data or related services rendered via such systems.[27] To ensure cybersecurity, an adequate level of protection of information systems needs to be provided. To this end, restrictions on civil liberties in cyberspace may occur in certain special cases. However, they may only be introduced on condition that such protection cannot be ensured otherwise.[28]

Cybersecurity and national cybersecurity system. Cybersecurity refers to information systems, i.e. the ICT systems through which electronic data is processed. These systems are widely used in the private and public sectors and, without their efficient functioning, the implementation of tasks and the provision of services would be either significantly hindered or entirely impossible.

---

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4.5.2016).

[27] Article 2 (4) of the Polish Act of 5 July 2018 on national cybersecurity system (consolidated |text, Journal of Laws 2023, item 913, as amended), hereinafter: NCSA. See also M. Karpiuk, J. Kostrubiec, *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1), p. 117.

[28] M. Czuryk, *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), p. 34.

Cybersecurity is one of the domains of security,[29] so it should entail measures aimed at preventing and responding to threats and at mitigating their consequences. Another important aspect of security is to analyse the causes and sources of threats, and to subsequently apply solutions offering protection against them. Regarding cybersecurity, these are threats occurring in cyberspace.

The objective of the Polish cybersecurity system, under Article 3 NCSA, is to ensure cybersecurity at the national level, including the uninterrupted provision of essential and digital services. This is to be achieved by ensuring the adequate level of security of the information systems used to provide these services, and by guaranteeing the proper handling of incidents occurring in the country.[30] As regards the provision of essential services, cybersecurity is very important not only for service providers and service recipients but also for the entire state and its security.[31] Another objective of the system, also expressly set by the legislator, is to ensure an uninterrupted provision of digital services. This also highlights their significance. Digital services (similar to essential services) are also of great importance for the efficient functioning of the state and society. In addition, they allow fast and efficient communication and facilitate contacts, including with public administration.[32] Digital service providers, therefore, have an important place in the national cybersecurity system and are obliged to cooperate with other actors engaged in the system, including operators of essential services. These providers are obliged not only to eliminate cyberthreats but also to protect against them and mitigate their consequences. In this context, the underlying obligation is to take

[29] Regarding security, see also J. Kostrubiec, M. Karpiuk, D. Tyrawa, *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2); M. Ciesielski, *Dyskurs o bezpieczeństwie a media*, "Cybersecurity and Law" 2024, no. 2; M. Karpiuk, *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1); M. Czuryk, *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4); W. Konaszczuk, A. Nogalski, *Use of Unmanned Aerial Vehicles for Combat Purposes: Selected Legal and Medical Aspects*, "Studia Iuridica Lublinensia" 2024, vol. 33(2); M. Karpiuk, *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1); M. Ciesielski, *Socjologia bezpieczeństwa jako subdyscyplina nauk o bezpieczeństwie*, "Cybersecurity and Law" 2019, no. 2; M. Karpiuk, T. Włodek, *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1).

[30] See also F. Radoniewicz, [in:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, eds. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, p. 52.

[31] M. Karpiuk, *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, p. 167. See also M. Czuryk, *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), p. 48.

[32] M. Czuryk, *The Legal Status of Digital Service Providers in the National Cybersecurity System*, "Cybersecurity and Law" 2024, no. 1, p. 40.

appropriate technical and organisational measures matching risks related to the emergence of cyberthreats to ensure the cybersecurity of provided digital services.[33]

Ensuring cybersecurity is of strategic importance for Poland. This will be achieved by raising the level of resilience to cyberthreats, increasing information protection in the public, military and private sectors, and promoting knowledge and good practices to enable citizens to protect their information better.[34] The ability to respond to cyber threats is to be achieved in both the public and private domains. As cyberspace is used to provide services in both these mutually interdependent sectors, all users must exercise security in their cyberspace operations.

The intensity of protecting cyberspace can vary, depending on the cyberthreats that occur or are likely to occur.[35] This is related to the costs generated by cybersecurity, especially given the need to protect strategic sectors against cyberthreats in a continuous manner, using modern ICT solutions to eliminate cybersecurity incidents and their consequences.

The fight against cyberthreats forms a core element of public policy. Given the extent of such threats and their impact, it is a national – rather local – policy priority. However, building resilience against cyber-attacks must be done comprehensively and must take into consideration local threats as well. Therefore, local and regional government bodies must have adequate legal instruments and the appropriate technical tools to counter these threats.

Cybersecurity incidents. The CERT Polska team, which operates within NASK structures and performs some of the tasks assigned to CSIRT NASK, is responsible for monitoring cybersecurity threats and incidents at the national level. This includes coordination of incident handling and recording processes. As stipulated in Article 2 (3) 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.

The statistical data used for analysing the incidents occurring countrywide comes from the annual reports on the operations of CERT Polska for 2019–2023. This time frame was adopted because the National Cybersecurity System Act had come into force in 2018, but the first full year of its implementation was 2019.

CERT Polska recorded 6,484 incidents in 2019, 10,420 in 2020 and 29,483 in 2021. The upward trend continued in 2022 and 2023, with 39,683 and 80,267 incidents recorded, respectively. The most common incident type, one that impacts

[33] M. Karpiuk, *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2), pp. 198–199.

[34] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2022, p. 20.

[35] C. Gaie, M. Karpiuk, *The Provision of E-Services by Public Administration Bodies and Their Cybersecurity*, [in:] *Transforming Public Services…*, p. 182.

or may adversely impact cybersecurity, was computer fraud, with 4,086, 8,310, 25,472, 35,009 and 75,917 cases reported annually in the analysed period.

Computer fraud accounted for a significant portion of all incidents. In terms of the number of incidents, it was followed by malware. CERT Polska recorded 969 incidents of malware use in 2019, 746 in 2020, 2,847 in 2021 and 3,409 in 2022. The upward trend was reversed in 2023, with 1,650 incidents recorded. Incidents involving offensive and illegal content were recorded in the following numbers: 812 in 2019, 371 in 2020, 311 in 2021, 308 in 2022 and 584 in 2023.

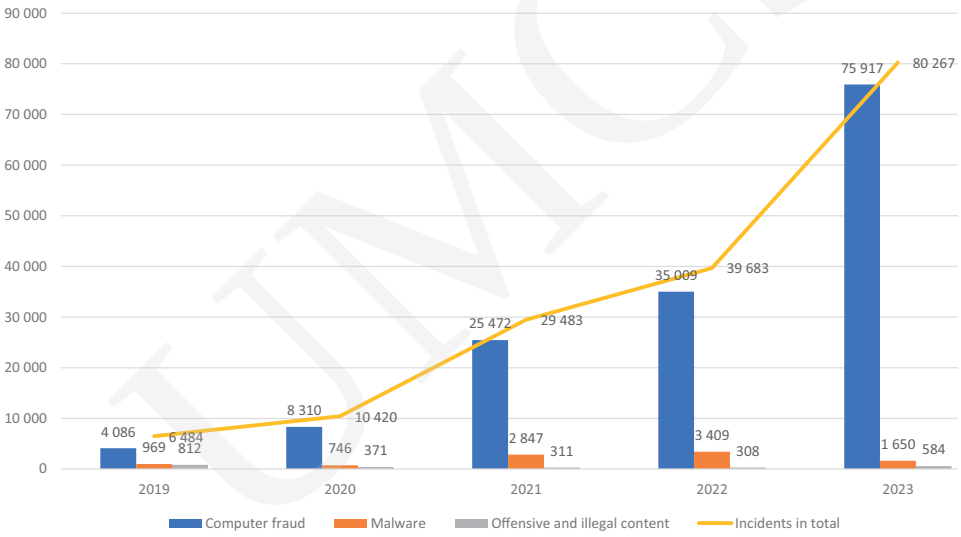

Figure 3. Number of incidents recorded by CERT Polska from 2019 to 2023 (by type)

Source: own elaboration based on annual reports on the operations of CERT Polska for 2019–2023.

Serious incidents form a category of incidents which entail severe consequences. Under Article 2 (7) NCSA, these are defined as incidents causing or likely to cause a serious deterioration in the quality or interruption of the continuity of an essential service. An essential service, under Article 2 (16) NCSA, is a service that is crucial to the maintenance of a critical social or economic activity. The importance of these services to both society and the economy is thus very high. Serious incidents, however, do not represent a large portion of all incidents in the analysed period. In 2019, there were 9 such incidents, in 2020 – 32, in 2021 – 36, in 2022 – 30, and in 2023 – 40.

CERT Polska records incidents not only by type but also by sector. In the case of public administration, 336 incidents were recorded in 2019, 388 in 2020 and 429 in 2021. In the following years, the upward trend continued, with 757 incidents recorded in 2022 and 2,234 in 2023. In the education and upbringing sector, 62, 71, 142, 167 and 354 incidents were recorded, respectively, in the consecutive years

of the analysed period. Regarding the healthcare sector, CERT Polska recorded the following number of incidents between 2019 and 2023: 53, 112, 150, 251, 405. As for digital infrastructure, 550 incidents were recorded in 2019, 1,016 in 2020, 1,606 in 2021 and 1,821 in 2022. The highest number of incidents in the digital infrastructure sector was recorded in 2023, i.e. 5,101 incidents.

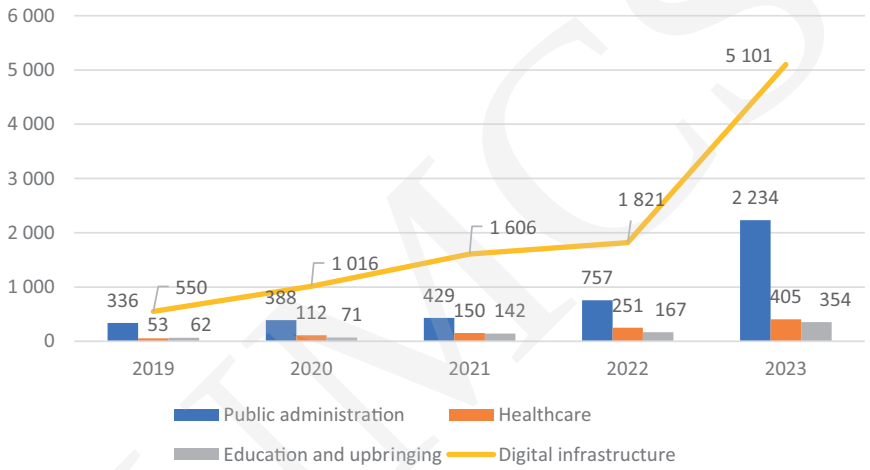

Figure 4. Number of incidents recorded by CERT Polska from 2019 to 2023 (by sector)

Source: own elaboration based on annual reports on the operations of CERT Polska for 2019–2023.

The Polish Cybersecurity Strategy highlights the need to increase the level of resilience to cyberthreats and the level of information protection in the public, military and private sectors. It also recognises the need to promote knowledge and good practices to better protect the information of individual society members. The following specific objectives are planned to be attained by Poland: developing a national cybersecurity system; increasing the level of resilience of information systems of public administration and the private sector, and providing the ability to prevent and respond to incidents effectively; increasing the national potential for ensuring security in cyberspace; building public awareness and competence in the area of cybersecurity; and building a strong international position of the Republic of Poland in the area of cybersecurity.[36]

[36] Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Polish Monitor 2019, item 1037).

CYBERSECURITY IN ITALY

In a continuously evolving cyber landscape, characterized by an increase in cyber-attacks (as evidenced by the latest Clusit Report,[37] which indicates that in 2023 attacks launched against Italy increased by 65% compared to those of the previous year), Italy has taken its first regulatory steps on cybersecurity in 2013, which was a relatively late development compared to other states. The DPCM Monti provided the country with an initial national architecture, which was revised first in 2017 with the so-called Decreto Gentiloni and later with DL 82/2021.

Over the past five years, Italy has strengthened its cyber defence capabilities through the establishment of the National Cybersecurity Agency (ACN), which was tasked with implementing the National Cybersecurity Strategy, formally unveiled in May 2022.

The objective of the following contribution is to analyze the Italian regulatory framework on cybersecurity, reconstructing the institutional architecture and the way Italy has addressed the challenges posed by the cyber domain.

The first national cybersecurity architecture. Italy's legislative approach to cybersecurity began in 2013 with the "DPCM Monti" of 24 January 2013.[38] The primary objective of the decree was to delineate for the first time an architectural framework for national cybersecurity and the protection of critical infrastructure. At the apex of the structure was the President of the Council of Ministers, who was responsible for adopting the National Strategic Framework for cyberspace security and the National Plan for national cyber protection and cybersecurity. The President was supported by the Comitato interministeriale per la sicurezza della Repubblica (CISR), which provided advice and regulatory and organizational proposals as part of its main functions. The CISR Tecnico provided support to the CISR in the execution of its activities. In addition, the decree assigned a significant role at the operational level to the Dipartimento delle Informazioni per la Sicurezza (DIS) and the various agencies (AISI, AISE, AgID). Furthermore, the decree established the Nucleo per la sicurezza cibernetico (NSC) within the office of the Consigliere Militare, which was tasked with supporting the President in matters pertaining to the prevention and preparation for potential crisis situations, as well as the activation of warning procedures. Finally, the institutional framework was further augmented by the inclusion of additional entities, including the NISP – Tavolo interministeriale di crisi cibernetica, the Scientific Committee, private operators, the Centro nazionale anticrimine infor-

[37] Clusit, *Rapporto sulla sicurezza ICT in Italia*, 2024, https://www.opificiumagazine.it/wp-content/uploads/2024/03/Rapporto-Clusit-2024.pdf (access: 4.5.2024).

[38] DPCM of 24 January 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg (access: 7.5.2024).

matico per la protezione delle infrastrutture critiche (CNAIPIC) and the Computer Emergency Response Team (CERTs) at the national, defense and PA levels.

Four years later, the DPCM Monti was revised by the so-called Decreto Gentiloni.[39] The new institutional set-up is motivated by two factors: the need to reduce complexity and the necessity of preparing for the transposition of the NIS Directive.[40]

The new structure includes the confirmation of the President of the Council of Ministers at the apex of the structure. The tasks of the CISR and the CISR Tecnico remain unchanged. The NSC has assumed a more central role within the nation architecture, no longer hosted by the Consigliere Militare but by the DIS. The NSC is chaired by a deputy director of the DIS and convenes on a monthly basis. Its primary function is to facilitate communication and collaboration between the various components of the institutional architecture. In contrast to the Monti Decree, the DPCM of 17 February 2017, in addition to reinforcing the role of the DIS, no longer provides the NISP – Tavolo interministeriale di crisi cibernetica and the Scientific Committee. Finally, the decree established a new Centro di Valutazione e Certificazione Nazionale (CVCN) within the Ministry of Economic Development, with the task of assessing the security of products and services for critical national infrastructure.

The Decree of 17 February 2017 also revised the National Plan[41] with the objective of providing immediate impetus to the further development phase of the national cyber architecture. Similarly to its predecessor, the revised National Plan comprises eleven operational guidelines, each with specific objectives and lines of action. The revision included a number of lines of action like: operational guideline 1 (Strengthening intelligence, police, and civil and military defense capabilities) was aligned with respect to the operational experience gained over the past two years in order to enhance overall capabilities for integrated response to cyber events; operational guideline 5 (Operationalization of national incident prevention, response and remediation structures) considered the need to strengthen existing CERTs, as well as the necessity to build the structures envisioned by the NIS Directive (CSIRT, single national point of contact, National Authority) and the manner in which to coordinate among the various actors in the architecture.

Recent developments – the National Cybersecurity Agency. The national legislative framework is once again regulated by DL 82/2021,[42] which establishes the

[39] DPCM of 17 February 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg (access: 7.5.2024).

[40] R. Baldoni, R. De Nicola, P. Prinetto, *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*, Roma 2018, p. 17.

[41] *Piano Nazionale per la protezione cibernetica e la sicurezza informatica*, 2017, https://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf (access: 7.6.2024).

[42] Decree-Law No. 182 of 14 June 2021, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg (access: 7.6.2024).

National Cybersecurity Agency: Agenzia per la cybersicurezza nazionale (ACN). The new authority is responsible for a number of key areas, including the National Cybersecurity Strategy, the coordination of cybersecurity activities among public actors at the national level, the implementation of measures to ensure cybersecurity and cybersecurity resilience for the development of Italian digitalization, the production system, and public administrations, as well as the promotion of national and European autonomy regarding IT products and processes of strategic importance to protect national interests in the field. The Agency is also the single point of contact for network and information system security under the NIS Directive, and is responsible for investigating breaches and imposing administrative sanctions.

In May 2022, ACN presented the National Cybersecurity Strategy 2022–2026[43] along with the Implementation Plan.[44] In order to meet the challenges poses by the cyber threat, the strategy identifies three key objectives (protection, response and development) and related measures, divided into thematic areas, to ensure its concrete implementation. Actions related to protection cover issues such as technology scrutiny, legal framework, situational awareness, cyber resilience of public administration, national infrastructure, encryption and countering disinformation. Crisis management, national cyber services, exercises, attribution, counter cybercrime and deterrence capabilities are the areas to which response-related efforts are directed. Finally, the development objective includes actions related to the Centro nazionale di coordinamento, national and European technology development, the Parco nazionale della sicurezza, cyber as a factor of competitiveness, and secure digitalization of the state.

Previously, a step forward from a national security perspective has been seen with the emergence of the "Perimetro di sicurezza cibernetico nazionale" through DL 105/2019[45] (converted into Law No. 133 of the same year). The legislation is aimed at entities, both public and private, that provide services or perform essential functions for the State in sectors considered to be most at risk (defence, energy, telecommunications, business and finance, transportation, critical technologies, etc.) and in need of enhanced security. Actors included in the perimeter are therefore required to adopt more stringent security measures, such as listing relevant ICT assets, notifying the CVCN of the purchase of ICT assets, systems and services, and notifying the CSIRT of any incidents related to ICT assets.

Cyberattacks – a brief overview. Analyses conducted by the Clusit 2024 Report on ICT security in Italy indicate a consistent increase, both qualitatively and quanti-

[43] *Strategia Nazionale di Cybersicurezza 2022–2026*, https://www.acn.gov.it/portale/documents/20119/87708/ACN_Strategia.pdf/6d98daf1-f3df-91e3-189d-df85f60402b6?t=1704461393347 (access: 9.6.2024).

[44] *Ibidem*.

[45] Decree-Law No. 105 of 21 September 2019, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica, https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/s (access: 9.6.2024).

tatively, of IT security incidents in Italy. Over the past five years, approx. 653 attacks of notable severity have been identified. Of these, 310 were recorded in 2023 alone, representing a 65% growth over the previous year's data. However, at the qualitative level, 43% of incidents had a high impact, the same percentage recorded for those with medium impact, 13% were classified as critical and 1% as low severity.

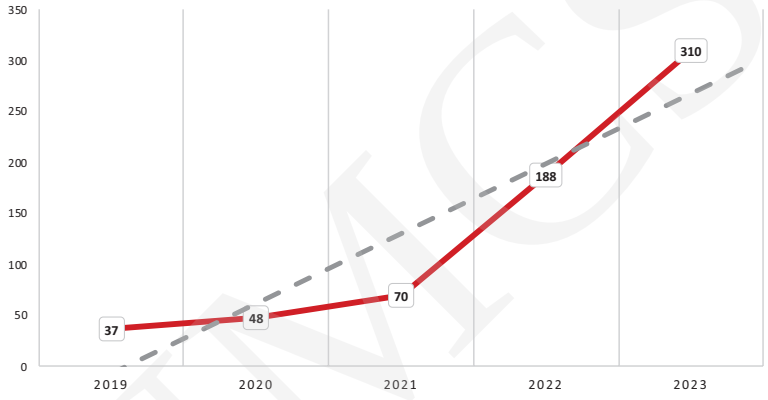

Figure 5. Cyber-attacks in Italy 2019–2023

Source: Clusit, *Rapporto sulla sicurezza ICT in Italia*, 2024, https://www.opificiumagazine.it/wp-content/uploads/2024/03/Rapporto-Clusit-2024.pdf (access: 4.5.2024), p. 34.

The Government sector is the most frequently targeted by cybercriminals (19%), followed by Manufacturing (13%), Transportation / Storage (12%), Multiple Targets (11%), Financial / Insurance (9%) and Wholesale / Retail (9%).

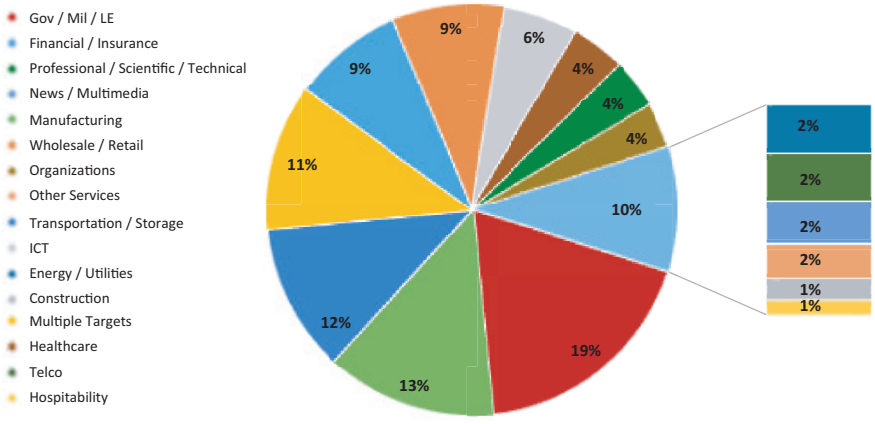

Figure 6. Distribution of the most affected sectors in Italy in 2023

Source: Clusit, *Rapporto sulla sicurezza ICT in Italia*, 2024, https://www.opificiumagazine.it/wp-content/uploads/2024/03/Rapporto-Clusit-2024.pdf (access: 4.5.2024), p. 38.

Distributed denial of service is the most commonly used 2023 attack technique (36%) to hit Italian businesses and institutions, with malware becoming less prevalent (dropping from 53% in 2022 to 33% in 2023).

Although Italy started to address national cybersecurity late compared to other states (e.g. France, the UK and Germany), it has at least managed to catch up with a national agency (ACN) and a renewed national cybersecurity strategy. The new national architecture, defined by DL 82/2019, represents an important development in addressing the challenges posed by the cyber domain. Nevertheless, the cyber domain is constantly evolving, as demonstrated by the data just mentioned, and it will only be possible to analyze the progress made when the National Strategy expires. What is certain is that the evolution of the cyber domain will not stop here, and therefore Italy must continue to be prepared in order not to lose all the work done so far.

CONCLUSIONS

The vast part of social activities has moved online. Therefore, ensuring digital security should be a fundamental task for public authorities. An information society is based on ICT systems that are not fully resistant to disruptions affecting such a society. Threats to information society have increasingly serious consequences, and cyber-attacks on these systems can be used as a means of political and economic pressure. The abundance of information surrounding humans and the dynamic development of information technologies are invariably changing every aspect of social, cultural, economic and political life.[46]

The society's digital transformation process, along with algorithm-based economy, poses challenges to the ongoing development of the state. It is noted that public, commercial and industrial services must accumulate huge amounts of data to be ready to enter the era of artificial intelligence. Data has become one of the most important production factors. This has become evident over the past few years. It has become a fundamental principle, governing economies and states, to acquire, collect, process and consciously use data, along with the development of artificial intelligence algorithms. This determines the place of individual states in the global supply chain and influences their development, determined by data processing in the fields where artificial intelligence comes into play.[47]

People must be at the heart of the digital transformation process. Technology should serve and benefit everyone in the EU. It should enable them to pursue their

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

[47] *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, Warszawa 2020, p. 8.

aspirations securely, with their rights and freedoms respected. Digital transformation should foster a fair and inclusive society and a fair economy in the EU, and everyone across the EU should have access to cheap and fast digital connectivity.[48]

Digital transformation creates new opportunities and forms of public participation and opinion-forming processes and exhibits the potential to engage the majority of members of societies. Digital technologies offer new ways of solving society's problems and increase the efficiency and effectiveness of public entities. Societies should take full advantage of the opportunities arising from digitisation. Digital technologies enable societies to combat instant and extreme threats. Importantly, innovative digital tools should be developed considering fundamental values and rights. However, this will only be possible if societies are properly skilled and have easy access to the necessary technology and connectivity.[49]

Both digital accessibility and digital competence are crucial. Digital accessibility, especially access to public services, allows easier and faster contact, including communication with public administration. It also enables many issues to be dealt with remotely, which appears particularly important for people having difficulty getting to an office. Digital competence enables the appropriate use of ICT tools in various areas of social or professional life. Due to the development of new technologies, the ability to use such tools is indispensable, as these technologies create opportunities for human development and determine progress in many spheres. Acquiring and expanding digital competence not only enables the optimal use of services provided in cyberspace but also contributes to reducing digital exclusion.

REFERENCES

Literature

Baldoni R., De Nicola R., Prinetto P., *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*, Roma 2018.

Bradshaw S., *Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*, London 2015, **DOI: https://doi.org/10.2139/ssrn.2700899**.

Ciesielski M., *Dyskurs o bezpieczeństwie a media*, "Cybersecurity and Law" 2024, no. 2, **DOI: https://doi.org/10.35467/cal/188577**.

Ciesielski M., *Socjologia bezpieczeństwa jako subdyscyplina nauk o bezpieczeństwie*, "Cybersecurity and Law" 2019, no. 2, **DOI: https://doi.org/10.35467/cal/133837**.

[48] European Declaration on Digital Rights and Principles for the Digital Decade (OJ C 23/1, 23.1.2023).

[49] Berlin Declaration on Digital Society and Value-Based Digital Government, https://www.gov.pl/web/cyfryzacja/cyfryzacja-oparta-na-wartosciach--podpisanie-deklaracji-berlinskiej (access: 21.5.2024).

Czuryk M., *Activities of the Local Government During a State of Natural Disaster*, "Studia Iuridica Lublinensia" 2021, vol. 30(4), **DOI: https://doi.org/10.17951/sil.2021.30.4.111-124**.

Czuryk M., *Cybersecurity and Protection of Critical Infrastructure*, "Studia Iuridica Lublinensia" 2023, vol. 32(5), **DOI: https://doi.org/10.17951/sil.2023.32.5.43-52**.

Czuryk M., *Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(3), **DOI: https://doi.org/10.17951/sil.2022.31.3.31-43**.

Czuryk M., *The Legal Status of Digital Service Providers in the National Cybersecurity System*, "Cybersecurity and Law" 2024, no. 1, **DOI: https://doi.org/10.35467/cal/187255**.

Gaie C., *Enhancing the Efficiency and the Security of E-Government: The French Case Study of Human Resources Applications*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024, **DOI: https://doi.org/10.1007/978-3-031-55575-6_10**.

Gaie C., Karpiuk M., *The Provision of E-Services by Public Administration Bodies and Their Cybersecurity*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024, **DOI: https://doi.org/10.1007/978-3-031-55575-6_7**.

Gaie C., Mueck M., *A Hybrid Blockchain Proposal to Improve Value-Added Tax Recovery*, "International Journal of Internet Technology and Secured Transactions" 2021, vol. 12(1), **DOI: https://doi.org/10.1504/ijitst.2022.119668**.

Hill R., *Dealing with Cyber Security Threats: International Cooperation*, Tallinn 2015, **DOI: https://doi.org/10.1109/CYCON.2015.7158473**.

Kaczmarek K., *Vulnerability to Cyber Threats: A Qualitative Analysis from Societal and Institutional Perspectives*, "Cybersecurity and Law" 2024, no. 2, **DOI: https://doi.org/10.35467/cal/188557**.

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

Kaczmarek K., Karpiuk M., Melchior C., *A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data*, "Prawo i Więź" 2024, no. 3.

Karpiuk M., *Glosa do wyroku Naczelnego Sądu Administracyjnego z dnia 12 lutego 2018 r. (II OSK 2524/17)*, "Studia Iuridica Lublinensia" 2019, vol. 28(1), **DOI: https://doi.org/10.17951/sil.2019.28.1.185-194**.

Karpiuk M., *Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level*, "Prawo i Więź" 2022, no. 4, **DOI: https://doi.org/10.36128/priw.vi42.524**.

Karpiuk M., *The Legal Status of Digital Service Providers in the Sphere of Cybersecurity*, "Studia Iuridica Lublinensia" 2023, vol. 32(2), **DOI: https://doi.org/10.17951/sil.2023.32.2.189-201**.

Karpiuk M., *The Provision of Safety in Water Areas: Legal Issues*, "Studia Iuridica Lublinensia" 2022, vol. 31(1), **DOI: https://doi.org/10.17951/sil.2022.31.1.79-92**.

Karpiuk M., Kostrubiec J., *Provincial Governor as a Body Responsible for Combating State Security Threats*, "Studia Iuridica Lublinensia" 2024, vol. 33(1), **DOI: https://doi.org/10.17951/sil.2024.33.1.107-122**.

Karpiuk M., Melchior C., Soler U., *Cybersecurity Management in the Public Service Sector*, "Prawo i Więź" 2023, no. 4, **DOI: https://doi.org/10.36128/PRIW.VI47.751**.

Karpiuk M., Włodek T., *Wygaśnięcie mandatu wójta na skutek skazania na karę grzywny za niedopełnienie obowiązków z zakresu zarządzania kryzysowego. Glosa do wyroku Sądu Rejonowego w P. z dnia 18 kwietnia 2019 r. (II K 1164/14)*, "Studia Iuridica Lublinensia" 2020, vol. 29(1), **DOI: https://doi.org/10.17951/sil.2020.29.1.273-290**.

Konaszczuk W., Nogalski A., *Use of Unmanned Aerial Vehicles for Combat Purposes: Selected Legal and Medical Aspects*, "Studia Iuridica Lublinensia" 2024, vol. 33(2), **DOI: https://doi.org/10.17951/sil.2024.33.2.129-147**.

Kostrubiec J., Karpiuk M., Tyrawa D., *The Status of Municipal Government in the Sphere of Ecological Security*, "Hungarian Journal of Legal Studies" 2024, vol. 65(2), **DOI: https://doi.org/10.1556/2052.2024.00510**.

Langlois-Berthelot J., Gaie C., Lebraty J., *Epidemiology Inspired Cybersecurity Threats Forecasting Models Applied to e-Government*, [in:] *Transforming Public Services – Combining Data and Algorithms to Fulfil Citizen's Expectations*, eds. C. Gaie, M. Mehta, Cham 2024, **DOI: https://doi.org/10.1007/978-3-031-55575-6_6**.

Luiijf H., Besseling K., Spoelstra M., Graaf P., *Ten National Cyber Security Strategies: A Comparison*, [in:] *Critical Information Infrastructure Security*, eds. S. Bologna, B. Hämmerli, D. Gritzalis, S. Wolthusen, Cham 2013, **DOI: https://doi.org/10.1007/978-3-642-41476-3_1**.

Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020, Warszawa 2020.

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

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2022.

Online sources

Clusit, *Rapporto sulla sicurezza ICT in Italia*, 2024, https://www.opificiumagazine.it/wp-content/uploads/2024/03/Rapporto-Clusit-2024.pdf (access: 4.5.2024).

Cybersecurity: International Cooperation Requires Reciprocity, 11.7.2019, https://www.banque-france.fr/en/publications-and-statistics/publications/cybersecurity-international-cooperation-requires-reciprocity (access: 28.5.2024).

Daniel M., *How Global Information Sharing Can Help Stop Cybercrime*, 8.6.2023, https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime (access: 4.6.2024).

Former et sensibiliser à la sécurité du numérique : un enjeu stratégique pour l'ANSSI, https://cyber.gouv.fr/actualites/former-et-sensibiliser-la-securite-du-numerique-un-enjeu-strategique-pour-lanssi (access: 28.5.2024).

La formation initiale en cybersécurité, https://cyber.gouv.fr/formation-initiale-en-cybersecurite (access: 28.5.2024).

National Strategic Review 2022, https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf (access: 28.5.2024).

Organisation de l'État français en gestion de crise cybernétique majeure, https://www.ihemi.fr/articles/organisation-de-letat-francais-en-gestion-de-crise-cybernetique-majeure (access: 18.5.2024).

Piano Nazionale per la protezione cibernetica e la sicurezza informatica, 2017, https://www.governo.it/sites/governo.it/files/piano-nazionale-cyber-2017.pdf (access: 7.6.2024).

Post-Quantum Cryptography: Six French Cyber Players Join Forces to Design the Secure Communication Networks of Tomorrow, 15.3.2024, https://www.thalesgroup.com/en/worldwide/security/press_release/post-quantum-cryptography-six-french-cyber-players-join-forces (access: 28.5.2024).

Presentation of the National Cyber-Strategy: 7 Projects Selected as Part of the Research Priority Readiness Program, 21.6.2022, https://www.cnrs.fr/en/press/presentation-national-cyber-strategy-7-projects-selected-part-research-priority-readiness (access: 28.5.2024).

SPARTA, *Re-Imagining the Way Cybersecurity Research, Innovation, and Training Are Performed in the European Union*, 26.2.20219, https://cyber.gouv.fr/sites/default/files/2019/02/communique-de-presse-sparta.pdf (access: 28.5.2024).

Strategia Nazionale di Cybersicurezza 2022–2026, https://www.acn.gov.it/portale/documents/20119/87708/ACN_Strategia.pdf/6d98daf1-f3df-91e3-189d-df85f60402b6?t=1704461393347 (access: 9.6.2024).

Stratégie nationale pour la sécurité du numérique, https://cyber.gouv.fr/sites/default/files/document/strategie_nationale_securite_numerique_fr.pdf (access: 10.5.2024).

The French Critical Infrastructures Information Protection (CIIP) Framework, https://cyber.gouv.fr/en/french-ciip-framework (access: 10.5.2024).
The French White Paper on Defence and National Security, 9.7.2008, https://www.europarl.europa.eu/cmsdata/175477/20080711ATT34025EN.pdf (access: 10.6.2024).
Un plan à 1 milliard d'euros pour renforcer la cybersécurité, 2021, https://www.info.gouv.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite (access: 18.5.2024).
What We Do, https://cyber.gouv.fr/en/what-we-do (access: 10.5.2024).

Legal acts

Berlin Declaration on Digital Society and Value-Based Digital Government.
Decree-Law No. 105 of 21 September 2019, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
Decree-Law No. 182 of 14 June 2021, Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.
DPCM of 17 February 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.
DPCM of 24 January 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.
European Declaration on Digital Rights and Principles for the Digital Decade (OJ C 23/1, 23.1.2023).
French Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (Data Protection Act).
Polish Act of 5 July 2018 on national cybersecurity system (consolidated text, Journal of Laws 2023, item 913, as amended).
Resolution No. 125 of the Council of Ministers of 22 October 2019 on the Cybersecurity Strategy of the Republic of Poland for 2019–2024 (Polish Monitor 2019, item 1037).
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119/1, 4.5.2016).

ABSTRAKT

Współcześnie cyberprzestrzeń jest tą sferą, która nie tylko zdominowała życie prywatne, lecz także w dużym stopniu jest wykorzystywana do prowadzenia działalności gospodarczej, w tym świadczenia usług, jak również do wykonywania zadań publicznych. Pozwala to na usprawnienie działalności, zarówno publicznej, jak i niepublicznej, redukowanie kosztów oraz zwiększenie dostępności dla odbiorców. Cyberprzestrzeń pozwala też na szybszą komunikację, jej znaczenie jest zatem bardzo duże. Wraz z rozwojem nowych technologii i powszechnym korzystaniem z Internetu nasilają się również cyberzagrożenia. Walka z nimi musi być wpisana nie tylko w działalność przedsiębiorcy czy aktywność użytkownika sieci, ale też w politykę publiczną, i to zarówno centralną, jak i realizowaną na szczeblu lokalnym i regionalnym. Odpowiednie zarządzanie cyberbezpieczeństwem pozwala na optymalne wykorzystanie cyberprzestrzeni oraz na przeciwdziałanie zagrożeniom w niej występującym.

Słowa kluczowe: cyberbezpieczeństwo; cyberprzestrzeń; oszustwa komputerowe; złośliwe oprogramowanie

Ministerstwo Nauki i Szkolnictwa Wyższego
Doskonała Nauka II

Projekt dofinansowany ze środków budżetu państwa, przyznanych przez Ministra Edukacji i Nauki w ramach Programu „Doskonała Nauka II"