DOMINIK BIERECKI, MIROSŁAW KARPIUK, MARTIN KELEMEN, SERGII PRYLIPKO

The Impact of Digital Transformation on Cybersecurity in Poland, Slovakia, and Ukraine*

Abstract

Digital transformation is becoming increasingly widespread, and it can be said that it is an inevitable process. Digitization has enabled the streamlining of a wide range of tasks, from simple everyday activities to complex operations, enhancing efficiency, speed, and cost-effectiveness in their execution. The degree of digitization in a country is a key indicator of its level of development and the competitiveness of its economy. However, the phenomenon of digitization necessitates a heightened focus on cybersecurity measures. Investment in solutions that guarantee cybersecurity is essential for the success of digital transformation, as new technologies are integral to such transformations and will be effectively exploited by cybercriminals and cyberterrorists

DOMINIK BIERECKI – associate professor, Pomeranian University in Slupsk (Poland), ORCID – 0000-0001-6993-3974, e-mail: dominik.bierecki@upsl.edu.pl
MIROSŁAW KARPIUK – full professor, University of Warmia and Mazury in Olsztyn (Poland), ORCID – 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl
MARTIN KELEMEN – assistant professor, Technical University in Kosice (Slovakia), ORCID – 0000-0003-1015-1112, e-mail: martin.kelemen@tuke.sk
SERGII PRYLIPKO – associate professor, State University of Trade and Economics (Ukraine), ORCID – 0000-0002-6116-328X, e-mail: s.prylipko@knute.edu.ua

* This article was written as part of an international research project titled "Security in the Digital Space," planned for 2025-2026. The following entities are partners in this project: Institute of Security Studies, University of Siedlce (Poland); Department of Public Administration, Management of Innovative Activities and Consulting, National University of Life and Environmental Sciences of Kyiv (Ukraine); Faculty of Aeronautics, Technical University of Kosice (Slovakia); Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn (Poland).

HTTPS://DOI.ORG/10.36128/WPPKHN68

if not protected. IT systems used in strategic sectors responsible for national or international security must be adequately protected (cybersecurity). Such systems must be resistant to cyberthreats.

KEYWORDS: cyberspace, cybersecurity, new technologies, artificial intelligence

1 Introduction

Digital transformation is a pervasive phenomenon that impacts nearly every aspect of life. Cyberspace is used in both everyday life and business, and it is also becoming increasingly important in the public sphere. Technological development and the integration of artificial intelligence tools have given rise to novel threats with significant implications for security. The virtual world has a profound impact on the real world, highlighting the imperative for robust cybersecurity measures. In today's digital age, cybersecurity has become a critical concern. On one side, we have the pervasive presence of the Internet and the extensive use of IT systems. On the other hand, we are confronted with the ongoing threat of cyberattacks. Cybersecurity is therefore intended to protect against unauthorized cyber interference, especially that which could limit the basic functions of the state (destabilize it), undermine the foundations of economic activity or hinder its conduct, and block the satisfaction of human cyber needs.

In the current era of technological development, artificial intelligence systems have the potential to provide valuable support in detecting and combating cyberattacks. AI has the potential to improve operational efficiency and reduce expenses, while also enhancing cybersecurity. As a technology of the future, artificial intelligence, when used properly, can serve to counter cyber threats, despite their diversity and dynamics. However, it is important to note that it can also contribute to the emergence of such threats. For this reason, it is essential to use it responsibly.[1] Artificial intelligence, encompassing advanced techniques, systems, and operational logic algorithms for data processing, is a promising area of development.

[1] Christophe Gaie, Mirosław Karpiuk, Nicola Strizzolo, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No. 6 (2024): 356-357.

The range of applications for artificial intelligence is broad, encompassing areas such as image, sound, and text analysis as well as advanced data processing that imitates human reasoning.[2]

Digital transformation cannot be considered in isolation from cybersecurity, which is essential for implementing and operating modern digital tools. Cybersecurity is defined as the activities necessary to protect networks, information systems, and their users from cyber threats.[3]

Digital transformation is largely determined by the use of artificial intelligence (AI) for many tasks. An artificial intelligence system is a machine system designed to operate with varying levels of autonomy after implementation. It can also demonstrate adaptability after implementation. For explicit or implicit purposes, it can infer how to generate outputs based on input data. These outputs can be recommendations, decisions, specific content, or predictions of future events that may affect the physical or virtual environment.[4]

---

2 *Productivity Strategy 2030* (Warszawa: MRiT, 2022), 65.

3 Article 2(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ EU L 151, pp. 15-69). For the definition of cybersecurity, see also: Małgorzata Czuryk, "Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica* Lublinensia, No. 5 (2023): 44-45; Ewa Maria Włodyka, Krzysztof Kaczmarek, "Cyber Security of Electrical Grids – A Contribution to Research" *Cybersecurity and* Law, No. 2 (2024): 262-263; Małgorzata Czuryk, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 35-39.

4 Article 3(1) of Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ EU L, p. 1689). The Artificial Intelligence Act aims to ensure that the European Union improves the functioning of the internal market by establishing a uniform legal framework for the development, placing on the market, making available and use of artificial intelligence systems. This is to be done in accordance with the values recognized by the European Union, with a view to promoting the widespread use of human-centric and trustworthy artificial intelligence, while ensuring a high level of protection of health, safety, fundamental rights (including democracy and the rule of law), and supporting innovation, Paweł Pelc, "Akt w sprawie sztucznej inteligencji," *Myśl Strategiczna*, No. 1 (2025): 36.

It should be emphasized that digital transformation is not an end in itself but rather an important element in ensuring the development of the state. Public administration, entrepreneurs, society, and non-governmental organizations should all be active participants in this process. The processes of digital transformation require the involvement of entities from both the public and private sectors. The state should be seen as an active participant in this process. It should not only support, but also stimulate, the use of new technologies. Adopting modern tools, including artificial intelligence, enables competition in various fields in a demanding international market.

The goal of this article is to demonstrate how digital transformation impacts cybersecurity in Poland, Slovakia, and Ukraine. The authors are not so much concerned with a thorough analysis of this impact as with highlighting certain problems related to it, especially those concerning cyber threats. The research methods used include the dogmatic-legal method and a literature review.

2 The Impact of Digital Transformation on Cybersecurity in Poland

Digital transformation requires the adoption of new technologies, affecting both the private sector, which is more open to technological changes that enable greater competitiveness, and the public sector, which is still accustomed to traditional forms of contact with citizens and traditional ways of doing things. Neither sector could operate effectively without technological development, which is why digital transformation is a necessity for a developed country and society.

The digital transformation of society and the economy through the use of algorithms is one of the major development challenges of the 21st century. In order to enter the era of artificial intelligence, public and commercial services as well as industry, must be deeply saturated with data. Acquiring, collecting, analyzing, processing, and consciously using data as well as continuously developing artificial intelligence algorithms, is becoming the foundation of economies and countries, determining their place in the global supply chain. The data-driven economy is changing existing development rules and providing opportunities for Polish entrepreneurs and

the Polish economy, because new solutions and services have only recently been developed and implemented. Societies that produce and effectively implement new solutions, especially in artificial intelligence, will be more developed than those that only use them.[5]

The processes that take place as part of the digital transformation must be adequately protected, and this protection is directly related to cybersecurity. As emphasized in the doctrine, an adequate level of cybersecurity enables entities (including the state) to function normally and greatly facilitates business activity.[6]

Cybersecurity requires a multifaceted analysis that takes into account not only IT infrastructure and digital skills, but also many other elements, including the security environment and the international situation.[7] Digital transformation cannot be considered in isolation from cybersecurity or international conditions because all these elements are interrelated. Cyberspace, which is used to conduct various types of activities (including economic, public, and social), is global in nature, not just national. According to Polish law, cyberspace is defined as the space for processing and exchanging information created by IT systems, along with the connections between them and the relationships with users.[8]

Digital changes require innovative, AI-based solutions. Such solutions cannot be implemented in an uncontrolled manner. Although autonomous systems are capable of operating without human intervention and in changing circumstances, they must be controlled because they can pose a major threat in both cyberspace and the real world. While they are synonymous with technological development, they can also give rise to new threats. Therefore, the human factor must influence their functioning.

---

5 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020* (Warszawa: KPRM, 2020): 8-9.

6 Mirosław Karpiuk, "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 190.

7 Krzysztof Kaczmarek, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 105-106.

8 Article 2(1b) of the Act of August 29, 2002, on martial law and the powers of the Commander-in-Chief of the Armed Forces and the principles of his subordination to the constitutional authorities of the Republic of Poland (consolidated text: Journal of Laws of 2025, item 504).

Artificial intelligence is a benchmark of technological progress.[9] Thanks to this progress, digital transformation is possible, and its effects are already visible in the Polish economy, particularly in the service sector.

Artificial intelligence occupies a prominent position in the field of new technologies. It can significantly contribute to ensuring an adequate level of security, including in cyberspace. However, it should be noted that appropriate safeguards must be put in place at the stage of creating artificial intelligence systems capable of analyzing data, making decisions, or learning independently to protect against misuse.[10]

Poland's prosperity largely depends on the growth of its economy and the success of its entrepreneurs. Artificial intelligence-based solutions present an opportunity to join the world's most prosperous countries. To this end, we must support the creation of Polish companies in this sector, integrate artificial intelligence solutions into everyday life, and promote collaboration between the private sector and public institutions in research and implementation. Increasing demand for Polish artificial intelligence solutions in public administration, state-owned companies, and the Armed Forces of the Republic of Poland is also important.[11]

It should also be noted that entrepreneurs should be supported in their efforts to adapt new digital technologies.[12] Without new technological solutions, they will not be competitive on the global market.

---

9 On the artificial intelligence, see also: Krzysztof Kaczmarek, "Sztuczna inteligencja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warszawa: ASzWoj, 2024), 250-252; Tomasz Gergelewicz, "Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas*, No. 2 (2024): 71-94; András Bencsik, "The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence" *Studia Iuridica Lublinensia*, No. 2 (2024): 14-17; Ewa Maria Włodyka, "Artificial Intelligence and Ecology: Sustainability in Local Management Concepts", [in:] *Ekologia w dyskursie. Sztuczna inteligencja*, ed. Daniel Kalinowski, Patryk Toczyński (Słupsk: UP, 2024), 309-340; Tomasz Gergelewicz, "Jailbreak – Unveiling Security Vulnerabilities of ChatGPT" *Ius et Securitas*, No. 2 (2025): 19-53; Krzysztof Kaczmarek, "Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją" *Cybersecurity and Law*, No. 1 (2021): 65-76; Ewa Maria Włodyka, "Artificial Intelligence as a Supporting Tool for Local Government Decision Making in Public Safety" *Defence Science Review*, No. 17 (2023): 80-91.

10 Pierre-Alexandre Boudy, Małgorzata Czuryk, Claudio Melchior, "The Use of New Technologies in the Field of Security" *Ius et Securitas*, No. 2 (2025): 68.

11 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, 32.

12 *Advancing the Digital Transformation of Polish Enterprises* (Brussels: EC, 2024), 94.

Digital transformation, including the new digital solutions used within its framework, affects not only the economy, but also society. Artificial intelligence, an important factor in digital transformation, is redefining many professions through automation and process optimization. As a result, machines are replacing routine and repetitive work. This exacerbates problems in socially excluded regions, increasing unemployment and creating various forms of inequality and discrimination. To include society in creating new professions in a data-driven economy, the state must create conditions that allow those at risk of losing their jobs due to artificial intelligence implementation to improve their skills in areas corresponding to market trends.[13]

Cybersecurity is essential for ensuring the proper functioning of artificial intelligence systems. The measures taken within this framework protect against the unauthorized modification of these systems and the use of these systems for illegal activities. Thus, these measures counteract threats.[14]

Digital transformation is about more than just implementing new digital technologies. It must also be accompanied by education that promotes the knowledge and skills necessary for properly using new digital technologies. This education must also build trust in these technologies and foster openness to the changes that accompany their introduction. Society must understand the processes of digital transformation, its benefits and risks, and how to adapt to the changes taking place.

Human capital, in the form of an educated society with strong skills in mathematics, logic, technical and natural sciences as well as creative thinking and teamwork, is the most important resource that has a significant impact on the development of new technologies, including artificial intelligence.[15]

Digital transformation requires developing a security policy that clearly emphasizes protecting important IT systems against threats that could disrupt their functioning and destabilize the state. Therefore, such a policy must focus on cybersecurity and be reflected in strategic documents. The need to protect cyberspace stems from Poland's security strategy, among other things. The strategy clearly states the need to increase resilience to

13 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, 22.

14 Dominik Bierecki, Christophe Gaie, Mirosław Karpiuk, "Artificial Intelligence in e-Administration" *Prawo i Więź*, No. 1 (2025): 386, 201.

15 *Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020*, 50.

cyber threats and the level of information protection in the public, military, and private sectors. It also emphasizes the importance of promoting knowledge and good practices that enable citizens to better protect their information. This goal can be achieved by developing cybersecurity skills, knowledge, and awareness among public administration staff and the general public, strengthening and expanding the state's potential through domestic cybersecurity solutions and state-funded research and development of new technologies, and cooperating with universities, scientific institutions, and enterprises in both the public and private sectors.[16]

3 The Impact of Digital Transformation on Cybersecurity in Slovakia

Digital transformation is an irreversible and pervasive process of integrating digital technologies into all spheres of social and economic life. For the countries of Central and Eastern Europe, including Slovakia, this process is not only an engine of innovation and economic growth, but also a source of unprecedented security challenges. The accelerated adoption of cloud services, the Internet of Things (IoT), artificial intelligence (AI), and massive data production are exponentially increasing the attack surface that can be exploited by state and non-state actors. Cyberattacks are no longer just a technical issue for IT departments; they have become a strategic threat to national security, economic stability and the very functioning of democratic institutions. This article provides an in-depth analysis of the impact of digital transformation on cybersecurity, with a primary focus on the Slovak Republic. It examines its strategic and legislative framework, the real threat landscape and vulnerabilities in key sectors.

The Slovak Republic, like other EU Member States, is aware that its prosperity and security are inextricably linked to its ability to protect its cyberspace. The state's approach is based on a multi-layered model that combines the highest policy strategies, dedicated action plans, legislation and operational capacity building.

16 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej* (Warszawa: BBN, 2020), 20.

The cornerstone of the state's approach is the Security Strategy of the Slovak Republic, adopted in 2021. This umbrella document, which defines the key security interests of the state, explicitly recognizes cyberspace as a new operational domain. Cyber attacks, together with hybrid threats and disinformation campaigns, are identified as a direct threat to the sovereignty, stability and democratic system of Slovakia.[17] The National Cyber Security Strategy for 2021-2025[18] is based on this highest strategic level. It is not just a declarative document, but a concrete plan that defines four main priorities:

1. state resilience: It focuses on the protection of critical infrastructure, the security of public authorities' networks and information systems, and capacity building to deal with large-scale cyber incidents;
2. trusted and secure cyberspace: This includes fighting cybercrime, protecting citizens' intellectual property and personal data;
3. collaboration, education, and support: It emphasizes building a functional ecosystem through public-private partnerships (PPPs), academia, and increasing security awareness and digital skills at all levels of education;
4. effective promotion of the interests of the Slovak Republic: Defines goals within the framework of international cooperation in the EU and NATO.

These strategic goals are legislatively anchored in Act No. 69/2018 Coll. on Cyber Security.[19] This Act, which originally transposed the NIS Directive, is undergoing a major amendment in response to the new, much stricter NIS2 Directive (EU) 2022/2555.[20] The implementation of the NIS2

17 Bezpečnostná stratégia Slovenskej republiky. https://www.mzv.sk/documents/10182/4694403/Bezpecnostna+strategia+SR_2021_SK_final.pdf. [accessed: 14.7.2025].

18 Národná stratégia a akčný plán kybernetickej bezpečnosti. https://www.nbu.gov.sk/612-sk/narodna-strategia-a-akcny-plan-kybernetickej-bezpecnosti/. [accessed: 14.7.2025].

19 Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/. [accessed: 17.7.2025].

20 Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Únii. https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32022L2555. [accessed: 17.7.2025].

Directive, which must be fully transposed by member states by October 2024, represents a revolutionary shift for Slovakia. It is estimated that the number of regulated entities in Slovakia will increase from a few hundred to approximately 7,000.[21] This brings with it several key challenges.

Supply chain security: NIS2 places particular emphasis on managing risks associated with third parties. Regulated entities will have to proactively vet and require their suppliers to comply with safety standards, which will create a cascading effect across the economy.[22]

Direct responsibility of management: The new legislation explicitly introduces the personal responsibility of top management for cybersecurity. Managers will have to undergo mandatory training and may be personally penalized for neglecting their duties, which represents a fundamental change in corporate culture.[23]

Shortage of experts: The massive expansion of duties faces the long-term problem of a shortage of qualified cybersecurity experts in Slovakia. This shortage can slow down the adoption of the necessary measures and increase costs for businesses.

Financial and administrative burden: Especially for small and medium-sized enterprises, which are newly regulated, the implementation of comprehensive security measures and the fulfilment of reporting obligations can be a significant burden.[24] Threats in Slovak cyberspace are specific and constantly evolving. The operational heart of defence is the National Security Authority (NSA)[25] [8], and its executive unit CSIRT.SK.[26] According

21 Smernica NIS2 sa bude týkať približne 7000 subjektov na Slovensku. https://www.alison-group.com/sk/blog/smernica-nis2-sa-bude-tykat-priblizne-7000-subjektov-na-slovensku. [accessed: 20.7.2025].

22 NIS2 a jej dopad na dodávateľské reťazce. https://www.taylorwessing.com/en/insights-and-events/insights/2023/10/nis2-and-its-impact-on-supply-chains. [accessed: 23.7.2025].

23 Smernica NIS2 a zákon o kybernetickej bezpečnosti. https://www.pwc.com/sk/sk/risk-assurance-slovensko/kyberneticka-bezpecnost/smernica-nis2.html. [accessed: 30.7.2025].

24 Smernica NIS2 sa bude týkať približne 7000 subjektov na Slovensku. https://www.alison-group.com/sk/blog/smernica-nis2-sa-bude-tykat-priblizne-7000-subjektov-na-slovensku.

25 NBÚ Národný bezpečnostný úrad. https://sita.sk/firmy-institucie/nbu/. [accessed: 5.8.2025].

26 Národná jednotka pre riešenie kybernetických bezpečnostných incidentov. https://www.csirt.sk/

to reports from security companies, such as ESET, which operate directly in Slovakia, the most common threats include:

- Spyware and data theft malware: The Central European region has long been dominated by threats such as Agent Tesla and Formbook, which are spread through phishing emails and are aimed at stealing login credentials and sensitive information from companies.[27]
- Ransomware: Attacks that encrypt data and demand a ransom continue to be one of the most destructive threats, with attackers increasingly employing a double-extortion model (the threat of publishing stolen data).
- Phishing and disinformation: Phishing attacks are becoming increasingly sophisticated (spear-phishing) and are often linked to disinformation campaigns aimed not only at financial gain, but also at polarizing society and undermining trust in state institutions.[28]

CSIRT.SK actively monitors these threats, issues alerts, coordinates incident resolution, and serves as a central point for mandatory reporting under the Cybersecurity Act. Vulnerabilities in key sectors of the digital transformation. Industry 4.0 and critical infrastructure: Slovakia, as an industrialized country with a dominant automotive sector, is investing massively in the automation and digitization of production. However, this intertwines the worlds of information technology (IT) and operational technology (OT). An attack on OT systems can cause not only financial losses, but also physical damage, production stoppage, or environmental disaster.[29]

Health: The digitalisation of health and the eHealth system have brought many benefits, but at the same time, they have created a centralised system containing extremely sensitive data on millions of citizens. A successful attack on the health sector could paralyze healthcare delivery and pose a huge privacy risk.[30]

---

27 ESET Threat Report T3 2023. https://www.welivesecurity.com/wp-content/uploads/2024/02/eset_threat_report_t32023.pdf. [accessed: 15.8.2025].

28 Bezpečnostná stratégia Slovenskej republiky. https://www.mzv.sk/documents/10182/4694403/Bezpecnostna+strategia+SR_2021_SK_final.pdf.

29 Národná stratégia kybernetickej bezpečnosti na roky 2021-2025. https://www.nbu.gov.sk/wp-content/uploads/2021/01/202101. [accessed: 19.8.2025].

30 NBÚ: Zdravotnícke zariadenia sú častým cieľom kybernetických útočníkov. https://www.nbu.gov.sk/sk/infoservis/aktuality/3419.html. [accessed: 27.8.2025].

Slovakia must consistently implement the strict requirements of the NIS2 Directive, which represents the largest legislative shift in this area in recent years. This will require not only technological investments, but above all, a change in thinking and corporate culture, with an emphasis on management responsibility and the security of the entire supply chain. The key to success will be to address the acute shortage of professionals through reforms in education, and to build a functional ecosystem in which the state, the private sector and academia work closely together. Only in this way can Slovakia ensure that its digital future is not only innovative and prosperous, but above all safe and resilient to threats that are increasingly sophisticated and dangerous.

4 The Impact of Digital Transformation on Cybersecurity in Ukraine

The state policy on digitalization and cybersecurity development in Ukraine is shaped by an extensive regulatory and legal framework, encompassing both foundational legislation in the field of information security and specialized acts aimed at fostering the digital economy and e-governance. The fundamental legal instruments include the Law of Ukraine "On the Protection of Information in Information and Communication Systems" (1994), the Law of Ukraine "On Electronic Documents and Electronic Document Management" (2003), the Law of Ukraine "On the State Service of Special Communications and Information Protection of Ukraine" (2006), the Law of Ukraine "On Personal Data Protection" (2010), the Law of Ukraine "On Electronic Identification and Trust Services" (2017), the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" (2017), the Law of Ukraine "On National Security of Ukraine" (2018), the Law of Ukraine "On Electronic Communications" (2020), the Law of Ukraine "On Public Electronic Registers" (2021), the Law of Ukraine "On the Specifics of Providing Public (Electronic Public) Services" (2021), the Law of Ukraine "On Cloud Services" (2022), and the Law of Ukraine "On the National Informatization Program" (2022). Equally significant are strategic documents, such as the Doctrine of Information Security of Ukraine (2017), the Concept for the Development of E-Governance (2017), the Concept for

the Development of the Digital Economy and Society (2018), the Concept for the Development of Digital Competences (2021), the Cybersecurity Strategy of Ukraine (2021), and the Strategy for the Development of the Electronic Communications Sector until 2030 (2025). Collectively, this body of legislation and strategy papers has established the legal and institutional foundations for shaping modern state policy on digitalization and cybersecurity.

Over the past decade, digital transformation has gradually become a key component of modernizing the system of public administration and an essential condition for enhancing the digital competences of civil servants. A significant confirmation of this trend is Ukraine's progress in international rankings: since 2018, the country has advanced by 97 positions, and in 2024 ranked 5th in the United Nations Online Services Index, reflecting substantial progress in the development of e-governance.[31] The central driver of these changes has been the Ministry of Digital Transformation of Ukraine, which has shaped contemporary policy in the areas of e-governance, digital services, open data, and digital literacy. The digital system "Diia" provides citizens with convenient access to administrative services: as of the end of 2024, the state portal offered 137 online services, while the mobile application enabled access to 93 services, including 62 public services and 31 electronic documents. At the same time, the development of digital infrastructure covers an extensive network of administrative service delivery points, comprising more than 5,000 access points across the country.[32] These achievements not only simplify citizen-state interaction, saving budgetary resources and time, but also contribute to greater efficiency in governance and transparency in the public sector.

On the one hand, the introduction of digital technologies and the automation of administrative processes ensure higher quality and speed in the provision of public services, create prerequisites for the effective functioning of e-governance, facilitate the systematization of large volumes of data in state registers, and reduce corruption risks. On the other hand, the full-scale armed aggression of the Russian Federation against Ukraine has triggered an unprecedented level of cyber threats, manifested in large-scale

31 *E*-Government Development Index. UN E-Government Knowledgebase. https://publicadministration.un.org/egovkb/Data-Center. [accessed: 22.9.2025].

32 Report on the Implementation of the Work Plan of the Ministry of Digital Transformation of Ukraine for 2024, 2025. https://surl.li/coldoa. [accessed: 22.9.2025].

and systemic attacks on the information resources of public authorities, the banking system, the energy sector, and other critical infrastructure facilities. The most widespread forms include DDoS attacks on government services and electronic portals, the use of malicious software to destroy or corrupt data as well as targeted phishing campaigns against state institutions. Such actions are not only technical but also political in nature: they are aimed at destabilizing the functioning of public authorities, undermining citizens' trust in digital services, gaining covert control over state registers, damaging or destroying critical information, conducting intelligence and subversive activities, and disabling critical infrastructure facilities. The scale and continuity of these attacks constitute a systemic threat to public administration, necessitating integrated response measures and strengthened international cooperation in the field of cybersecurity.

Since the beginning of the full-scale aggression of the Russian Federation in 2022, Ukrainian legislation has undergone significant changes aimed at strengthening cybersecurity and enhancing the resilience of state institutions. A major step was the adoption in March 2025 of the Law of Ukraine "On Amendments to Certain Laws of Ukraine on the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects," which substantially updated the provisions of the foundational Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine."[33] The expanded understanding of cybersecurity introduced by this act encompasses a complex of organizational, legal, engineering and technical, cryptographic, and technological measures designed to ensure the resilience, integrity, availability, and confidentiality of information resources in cyberspace. This approach strengthens the protection of state information systems and critical infrastructure, while increasing the capacity of public administration to respond to cyberattacks and to adapt to the growing challenges of hybrid warfare.

The national cybersecurity system of Ukraine operates on the basis of interaction among several central state institutions, including the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Police of Ukraine, the Ministry of Defense of Ukraine and the General Staff of the Armed Forces, intelligence agencies, the National Bank of Ukraine, and the Ministry of

33 On the Basic Principles of Ensuring Cybersecurity of Ukraine. Law of Ukraine of 5 October 2017 No. 2163-VIII. https://zakon.rada.gov.ua/laws/show/2163-19#Text. [accessed: 22.9.2025].

Foreign Affairs of Ukraine. A central role in ensuring their coordination is performed by the National Cybersecurity Coordination Center under the National Security and Defense Council of Ukraine, which organizes responses to cyber incidents, attacks and threats, and provides strategic planning in the field of cyber defense. In addition, the law establishes requirements for the creation of cybersecurity units and the appointment of their heads within those public authorities that own or manage information, electronic communications, information and communication systems. These measures are aimed at strengthening the institutional capacity of the public sector to counter cyber threats, and at shaping a multi-level system of cybersecurity.

Under martial law, the Ministry of Digital Transformation of Ukraine has become a key coordinator in ensuring the country's digital resilience. Its activities encompass the preservation and migration of state registers to secure cloud services provided by international companies, the organization of cooperation with partners in the field of cybersecurity to repel large-scale attacks as well as the implementation of digital education programs and the promotion of cyber literacy among citizens and civil servants. The Ministry ensures the continuity of state digital platforms, coordinates interaction with the private sector in the field of cybersecurity, and introduces modern standards of information protection into public administration. Through international partnerships with the EU, NATO, and leading IT companies, state registers have been transferred to protected cloud environments, thereby strengthening national cyber defense capabilities. Notably, even during the most massive cyberattacks, the state portal and the mobile application "Diia" continued to operate, providing citizens with access to essential public services, and thereby sustaining trust in state institutions.

To ensure proper coordination and rapid response to cyberattacks, the Ministry of Digital Transformation of Ukraine actively engages the resources of international partners. An important step in this direction was the establishment, in 2023, of the Tallinn Mechanism – a multilateral initiative involving Ukraine and leading states of Europe and North America, aimed at consolidating efforts in the field of cybersecurity. The mechanism is designed to coordinate international assistance for the protection of critical infrastructure, the enhancement of cyber resilience, and the countering

of Russian cyberattacks.[34] To implement its tasks, in 2024, Ukraine established an Interagency Working Group responsible for aligning the actions of public authorities with international partners and facilitating the implementation of technical assistance projects.[35] Within this initiative Denmark, Estonia, France, Germany, the Netherlands, Poland, Sweden, the United Kingdom, Canada, and the United States provide ongoing support to Ukraine directed at strengthening national security and preventing Russian cyber threats. For example, over the next two years, Canada will invest 3 million Canadian dollars in the development of defense systems and equipment for detecting and preventing cyberattacks. [36] In 2025, Norway also joined the mechanism, announcing funding of more than 25 million Norwegian kroners for projects to enhance the cyber resilience of critical and civil infrastructure.[37] Thus, the Tallinn Mechanism has become an important instrument for integrating Ukraine into the international cybersecurity system and ensuring its long-term digital resilience.

One example of international support for Ukraine's digital resilience is the DT4UA (Digital Transformation for Ukraine) project, financed by the European Union and implemented by the e-Governance Academy (Estonia) in cooperation with the Ministry of Digital Transformation of Ukraine. Within the framework of this project, since 1 January 2025, enhanced information protection has been introduced for the subsystem monitoring access to personal data in the electronic interaction system of state electronic information resources "Trembita." The development of the new

34 Tallinn Mechanism: Ukraine and International Partners Launched a New Instrument of Cooperation in Cyberspace. Ministry of Foreign Affairs of Ukraine. https://mfa.gov.ua/news/tallinnskij-mehanizm-ukrayina-ta-mizhnarodni-partneri-zapochatkuvali-novij-instrument-spivpraci-u-kiberprostori. [accessed: 22.9.2025].

35 On the Establishment of the Interagency Working Group on Attracting International Assistance to Ensure the Cybersecurity and Cyber Resilience of the State: Resolution of the Cabinet of Ministers of Ukraine of 8 March 2024 No. 276. https://zakon.rada.gov.ua/laws/show/276-2024-п#Text. [accessed: 22.9.2025].

36 Canada to Allocate Approximately 92 Million UAH (3 Million CAD) to Support the Implementation of Projects within the Tallinn Mechanism. Ministry of Digital Transformation of Ukraine. https://thedigital.gov.ua/news/kanada-vidilyae-92-mln-grn-na-posilennya-kiberstiykosti-ukraini. [accessed: 22.9.2025].

37 Norway Became the Twelfth Country to Join the Tallinn Mechanism—an International Initiative Supporting the Strengthening of Ukraine's Cybersecurity. Ministry of Digital Transformation of Ukraine. https://thedigital.gov.ua/news/norvegiya-priednalas-do-tallinnskogo-mekhanizmu-dlya-pidtrimki-kiberstiykosti-ukraini. [accessed: 22.9.2025].

version "Trembita 2.0", is aimed at increasing the performance and security of data exchange between state registers as well as optimizing mechanisms for protecting sensitive information – an element of critical importance for the stability of e-governance under martial law. [38]

An important dimension of international cooperation is the enhancement of civil servants' digital literacy and their preparation for countering cyber threats. In February 2025, the project Cybersecurity Capacity Building for Ukraine (CCBU) was launched, initiated by France within the framework of the Tallinn Mechanism and financed by the French Ministry of Foreign Affairs through the mAIDan Facility Ukraine program. With the support of Expertise France, twenty specialized training sessions are planned by the end of 2025, aimed at strengthening cyber resilience and implementing international standards in the field of cybersecurity.[39] In parallel, in May 2025, the National Agency of Ukraine on Civil Service, in cooperation with the Higher School of Public Administration, the State Service of Special Communications and Information Protection of Ukraine and with the support of the EU project EU4PAR 2 launched an advanced training program on cybersecurity for heads of information security units, IT departments of public authorities, and deputy heads for digital development (CDTOs). The training program consists of four modules dedicated to legislative changes, strategies for responding to cyber incidents, the integration of European standards (in particular, NIS2), and the use of innovative technologies.[40]

Despite substantial progress in digitalization and the strengthening of cybersecurity, significant challenges remain within Ukraine's public authorities. The most critical is the shortage of qualified personnel in the field of cybersecurity, largely due to the mobilization of the male population into the Armed Forces of Ukraine as well as the comparatively low salaries in the public sector relative to the private IT industry. This reduces

38 DT4UA. Digital solutions that change Ukraine. https://ega.ee/wp-content/uploads/2025/05/dt4ua_brochure_en.pdf?utm_source=chatgpt.com. [accessed: 25.9.2025].

39 France and Ukraine Unite to Enhance Cybersecurity Capacity. EU4DIGITAL. https://eufordigital.eu/france-and-ukraine-unite-to-enhance-cybersecurity-capacity/?utm_source=chatgpt.com. [accessed: 27.9.2025].

40 The National Agency of Ukraine on Civil Service Launched a Cybersecurity Training Program for CDTOs of Public Authorities. NAUCS. https://nads.gov.ua/news/u-nads-startuvala-navchalna-prohrama-z-kiberzakhystu-dlia-cdto-derzhavnykh-orhaniv. [accessed: 30.9.2025].

the capacity of state institutions to effectively respond to sophisticated cyberattacks and to implement preventive measures. An additional challenge is limited funding which does not allow for the timely modernization of outdated information and communication systems, the deployment of comprehensive solutions, or the adoption of innovative technologies, including those based on artificial intelligence. The issue of training and retraining cybersecurity specialists requires further development, as it directly determines the pace of integration of European standards and practices, and the overall level of cyber resilience in public administration. Furthermore, insufficient intensity in drafting the necessary documents for full harmonization of Ukrainian legislation with European norms in the field of cybersecurity slows Ukraine's integration into the unified European cyberspace and creates additional challenges on its path toward EU membership. Taken together, these factors pose a serious threat to the stable functioning of public authorities and to sustaining citizens' trust in digital public services under the conditions of Russia's hybrid aggression.

Addressing these challenges requires a comprehensive approach. Foremost, this concerns the systematic training and retraining of personnel for cybersecurity units within public authorities. Equally important is the creation of motivational mechanisms to attract and retain specialists, including through improving the remuneration system, organizing internships for young IT professionals in leading foreign companies, and introducing additional incentives for civil servants working in the field of cybersecurity.[41] Particular attention should be given to ensuring adequate funding for the modernization of technical infrastructure and the implementation of innovative solutions, including artificial intelligence technologies. No less significant is the task of integrating European standards, in particular NIS2, into the functioning of the public sector. At the same time, it is essential to expand public-private partnerships in the field of cybersecurity and to strengthen cooperation with international organizations in order to enhance the cyber resilience of state institutions.

Thus, Ukraine's experience demonstrates that digital transformation and cybersecurity are interrelated processes which, under martial law, acquire critical importance for ensuring national security. The effective combination of innovative technologies, regulatory frameworks, institutional

41 Nataliia Vasylieva, Oleksandra Vasylieva, Sergii Prylipko, Svitlana Kapitanets, „Approaches to the Formation of Public Administration in the Context of Decentralization Reform in Ukraine" *Cuestiones Políticas*, No. 38 (2020): 301-320.

cooperation, and systemic international support establishes the essential conditions for strengthening the resilience of public administration and enhancing its capacity to counter cyber threats originating from the Russian Federation.

5 Conclusion

Implementing modern technological solutions is essential to ensuring an adequate level of security.[42] Such solutions must provide adequate protection against threats, including those in cyberspace, without generating threats themselves. Focusing on new technologies means focusing on cybersecurity. Investing in modern solutions that support the digitization process must be accompanied by adequate cybersecurity funding.

In a digital state, managing cyberspace, including cybersecurity, is important. Cybersecurity management should take into account the principle of minimizing disruption to IT systems which is also related to the justified restriction of access to these systems for users. Implementing this principle should facilitate the rapid detection of defects in a given IT system and prevent the irreversible destruction of processed data. One objective of this management is identifying vulnerabilities in IT systems that could be exploited for cyberattacks. This management should result in conclusions and guidelines that enable the prevention of threats, their early detection, and the minimization of their effects.[43]

Sometimes, ensuring cybersecurity requires restricting human rights and civil liberties.[44] However, this will not always be possible, especially when cybersecurity is clearly more important than human and civil liberties and rights. It should be emphasized that such restrictions must be

42 Mirosław Karpiuk, "Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź,* No. 4 (2022): 178.

43 Mirosław Karpiuk, Claudio Melchior, Urszula Soler, "Cybersecurity Management in the Public Service Sector" *Prawo i Więź,* No. 4 (2023): 23.

44 On the subject of restrictions on individual freedoms and rights, see Małgorzata Czuryk, "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd" *Studies in Religious Law,* No. 27 (2024): 158; Małgorzata Czuryk, "Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 119-121.

reasonable, and must end once the cybersecurity threat has passed or its effects have been mitigated.

As new technologies develop and cyberspace is used to provide services, cyber threats can cause crises. This is exacerbated by the fact that such threats are highly dynamic and diverse. Due to their intensity, particularly when they occur in strategic areas of state activity and important economic sectors, crisis management in the cybersecurity environment requires special attention.[45] Effective crisis management in cybersecurity is essential for a successful digital transformation, as the effects of cyberattacks can undermine national security.

However, it should be noted that society's dependence on universal access to information and network services poses several risks, such as limited access to services in the event of telecommunications infrastructure failure, or disinformation.[46] Living in a world where media and new technologies significantly impact modern societies means we can communicate more easily, access information, and have greater knowledge. At the same time, we should recognize the problems associated with modern technological achievements. First, communication via the internet is changing traditional forms of threats. New social pathologies, dysfunctions, and problems are emerging, especially social ones.[47]

---

45 Małgorzata Czuryk, "Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 6. Regarding crisis management, see also: Małgorzata Czuryk, "Jurisdiction of the Voivode in the Field of Crisis Management" *Studia Iuridica Lublinensia*, No. 2 (2025): 87-98.

46 Tomasz Wojciechowski, "Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego" *Ius et Securitas*, No. 1 (2024): 85. On the subject of disinformation, see also: Krzysztof Kaczmarek, "Russian Disinformation as an Element of Influence Building in Europe: Analysis and Perspectives" *Roczniki Nauk Społecznych*, No. 1 (2024): 109-121; Bogdan Grabowski, "Cyfrowe zagrożenia – zarys problemu" *Ius et Securitas*, No. 1 (2024): 100-102; Krzysztof Kaczmarek, "Consequences of Disinformation: An Overview of Selected Tools and Techniques of Manipulation" *National Security*, No. 2 (2024): 11-27; Tomasz Gergelewicz, "Countering Disinformation Concept for Building Social Resilience in Times of Cognitive Warfare" *Defence Science Review,* No. 20 (2024): 31-44. https://doi.org/10.37055/pno/200300; Krzysztof Kaczmarek, "Disinformation as a Risk Factor in Crisis Situations" *Roczniki Nauk Społecznych*, No. 2 (2023): 19-30; Maciej Ciesielski, "Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities" *Cybersecurity and Law,* No. 1 (2024): 190-197.

47 Andrzej Pieczywok, "Wirtualna przestrzeń edukacji człowieka" *Ius et Securitas*, No. 1 (2025): 53.

Bibliography

Bencsik András, "The Opportunities of Digitalisation in Public Administration with a Special Focus on the Use of Artificial Intelligence" *Studia Iuridica Lublinensia*, No. 2 (2024): 11-23. https://doi.org/10.17951/sil.2024.33.2.11-23.

Bierecki Dominik, Gaie Christophe, Karpiuk Mirosław, "Artificial Intelligence in e-Administration" *Prawo i Więź*, No. 1 (2025): 387-407. https://doi.org/10.36128/PRIW.VI54.1201.

Boudy Pierre-Alexandre, Czuryk Małgorzata, Melchior Claudio, "The Use of New Technologies in the Field of Security" *Ius et Securitas*, No. 2 (2025): 67-78.

Ciesielski Maciej, "Disinformation in Cyberspace. Introduction to Discussion on Criminalisation Possibilities" *Cybersecurity and Law*, No. 1 (2024): 185-199.

Czuryk Małgorzata, "Activities of the Local Government During a State of Natural Disaster" *Studia Iuridica Lublinensia*, No. 4 (2021): 111-124. https://doi.org/10.17951/sil.2021.30.4.111-124.

Czuryk Małgorzata, "Cybersecurity and Protection of Critical Infrastructure" *Studia Iuridica Lublinensia*, No. 5 (2023): 43-52. https://doi.org/10.17951/sil.2023.32.5.43-52.

Czuryk Małgorzata, "Dopuszczalne różnicowanie sytuacji pracowników ze względu na religię, wyznanie lub światopogląd" *Studies in Religious Law*, No. 27 (2024): 151-163. https://doi.org/10.31743/spw.17518.

Czuryk Małgorzata, "Jurisdiction of the Voivode in the Field of Crisis Management" *Studia Iuridica Lublinensia*, No. 2 (2025): 87-98. https://doi.org/10.17951/sil.2025.34.2.87-98.

Czuryk Małgorzata, "Restrictions on the Exercising of Human and Civil Rights and Freedoms Due to Cybersecurity Issues" *Studia Iuridica Lublinensia*, No. 3 (2022): 31-43. https://doi.org/10.17951/sil.2022.31.3.31-43.

Czuryk Małgorzata, "Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa" *Ius et Securitas*, No. 1 (2025): 5-12.

Gaie Christophe, Karpiuk Mirosław, Strizzolo Nicola, "Cybersecurity of Public Sector Institutions" *Prawo i Więź*, No. 6 (2024): 347-362. https://doi.org/10.36128/PRIW.VI53.1129.

Gergelewicz Tomasz, "Bipolarity of Artificial Intelligence – Chances and Threats" *Ius et Securitas*, No. 2 (2024): 71-94.

Gergelewicz Tomasz, "Countering Disinformation Concept for Building Social Resilience in Times of Cognitive Warfare" *Defence Science Review*, No. 20 (2024): 31-44. https://doi.org/10.37055/pno/200300.

Gergelewicz Tomasz, "Jailbreak – Unveiling Security Vulnerabilities of ChatGPT" *Ius et Securitas*, No. 2 (2025): 19-53.

Grabowski Bogdan, "Cyfrowe zagrożenia – zarys problemu" *Ius et Securitas*, No. 1 (2024): 95-105.

Kaczmarek Krzysztof, "Consequences of Disinformation: An Overview of Selected Tools and Techniques of Manipulation" *National Security*, No. 2 (2024): 11-27. https://doi.org/10.59800/bn/196693.

Kaczmarek Krzysztof, "Disinformation as a Risk Factor in Crisis Situations" *Roczniki Nauk Społecznych,* No. 2 (2023): 19-30. https://doi.org/10.18290/rns2023.0017.

Kaczmarek Krzysztof, "Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją" *Cybersecurity and Law*, No. 1 (2021): 65-76.

Kaczmarek Krzysztof, "Russian Disinformation as an Element of Influence Building in Europe: Analysis and Perspectives" *Roczniki Nauk Społecznych*, No. 1 (2024): 109-121. https://doi.org/10.18290/rns2024.0002.

Kaczmarek Krzysztof, "Sztuczna inteligencja", [in:] *Leksykon cyberbezpieczeństwa*, ed. Katarzyna Chałubińska-Jentkiewicz (Warszawa: ASzWoj, 2024): 250-252.

Kaczmarek Krzysztof, Mirosław Karpiuk, Claudio Melchior, "A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data" *Prawo i Więź*, No. 3 (2024): 103-121. https://doi.org/10.36128/PRIW.VI50.907.

Karpiuk Mirosław, "Recognising an Entity as an Operator of Essential Services and Providing Cybersecurity at the National Level" *Prawo i Więź* No. 4 (2022): 166-179. https://doi.org/10.36128/priw.vi42.524.

Karpiuk Mirosław, "The Legal Status of Digital Service Providers in the Sphere of Cybersecurity" *Studia Iuridica Lublinensia*, No. 2 (2023): 189-201. https://doi.org/10.17951/sil.2023.32.2.189-201.

Karpiuk Mirosław, Claudio Melchior, Urszula Soler, "Cybersecurity Management in the Public Service Sector" *Prawo i Więź*, No. 4 (2023): 7-27. https://doi.org/10.36128/PRIW.VI47.751.

Pelc Paweł, "Akt w sprawie sztucznej inteligencji" *Myśl Strategiczna*, No. 1 (2025): 35-46.

Pieczywok Andrzej, "Wirtualna przestrzeń edukacji człowieka" *Ius et Securitas*, No. 1 (2025): 53:64.

Vasylieva Nataliia, Oleksandra Vasylieva, Sergii Prylipko, Svitlana Kapitanets, „Approaches to the Formation of Public Administration in the Context of Decentralization Reform in Ukraine" *Cuestiones Políticas*, No. 38 (2020): 301-320. https://doi.org/10.46398/cuestpol.38e.19.

Włodyka Ewa Maria, "Artificial Intelligence and Ecology: Sustainability in Local Management Concepts", [in:] *Ekologia w dyskursie. Sztuczna inteligencja*, eds. Daniel Kalinowski, Patryk Toczyński. 309-340. Słupsk: UP, 2024.

Włodyka Ewa Maria, "Artificial Intelligence as a Supporting Tool for Local Government Decision Making in Public Safety" *Defence Science Review*, No. 17 (2023): 80-91. https://doi.org/10.37055/pno/185616.

Włodyka Ewa Maria, Krzysztof Kaczmarek, "Cyber Security of Electrical Grids – A Contribution to Research" *Cybersecurity and Law*, No. 2 (2024): 260-272.

Wojciechowski Tomasz, "Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego" *Ius et Securitas*, No. 1 (2024): 83-94.