Journal of Information Systems Engineering and Management
2025, 10(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Managing Cybersecurity Risks in the Era of Digital Transformation

Serhii Lysenko[1,*], Olha Verba[2], Viktor Kyrychenko[3], Vitaliy Gandziuk[4], Iryna Odobetska[5]

[1]*Doctor of Law, Professor, Director Institute of Security, Interregional Academy of Personal Management, Kyiv, Ukraine*
[2]*Candidate of Juridical Sciences, Docent, Associate Professor of the Department of Civil Law Disciplines, Institute of Law, Lviv State University of Internal Affairs, Lviv, Ukraine*
[3]*Candidate of Physical and Mathematical Sciences, Assistant Professor, Department of Computer Science, Faculty of Information Technologies, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine*
[4]*Candidate of Sciences in Social Communications, Associate Professor, Associate Professor of Department of Journalism, Advertising and Public Relations, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine*
[5]*Assistant of Department of Journalism, Advertising and Public Relations, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine*
** Corresponding Author: crimeconsult@ukr.net*

ARTICLE INFO

Received: 12 Oct 2024

Revised: 12 Dec 2024

Accepted: 23 Dec 2024

ABSTRACT

Introduction: The issue of information security risk management in digital transformations is of particular relevance given the increasing number and scale of threats to cybersecurity, electronic services, information systems and telecommunications networks. In this context, it is essential to ensure the effective integration of modern analysis tools, the introduction of innovative technologies and the formation of an appropriate regulatory framework capable of adapting to the modern digital environment.

Objectives: The article aims to systematise the key aspects of information security risk management in digital transformations.

Methods: The study used several general scientific methods of knowledge, including case analysis, systematisation and generalisation, regulatory framework, statistical data analysis, and Paired Samples T-Test using JASP software to assess the relationships between key indicators of digital infrastructure and cybersecurity.

Results: The t-test results revealed a statistically significant impact of digital transformation on critical aspects of cybersecurity. In particular, the development of e-governance ($t = 4.515$, $p = 0.02$) and access to online services ($t = 5.266$, $p = 0.013$) significantly increase the effectiveness of digital services protection and the ability to manage cyber crises, while the improvement of telecommunications infrastructure ($t = 3{,}314$, $p = 0.045$) contributes to the resilience of information systems during crises, especially in the context of modern cyber warfare, which underscores the critical role of digitalisation in strengthening national cybersecurity.

Conclusions: Thus, the analysis has revealed the need for a comprehensive approach to information security based on resilience, innovation, and international cooperation as crucial elements in countering modern cyber threats, especially in the Ukrainian context, which is against the backdrop of ongoing cyber warfare.

Keywords: information security, information infrastructure, cybersecurity, cyberwarfare, digitalisation, protection of individual rights, data protection in enforcement proceedings.

INTRODUCTION

Information security risk management is critical in today's rapid digital transformation of economic, social and technological systems. The digitalisation of the information ecosystem is accompanied by innovative technologies, such as large databases, blockchain, hybrid forms of organisational activity, digital platforms and national information infrastructure, which significantly change the nature of social relations. At the same time, e-commerce and automation systems are becoming more widespread, which, in addition to their positive impact, create favourable

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

conditions for cyberattacks and, therefore, require a comprehensive approach to their assessment and management. The growing amount of data processed and stored in digital systems keeps the possibility of confidential information leakage, data loss due to malware or system disruption due to cyberattacks alive. The availability of unlicensed software, the demonstration of a comprehensive state policy in the field of information security, and the escalation of cybercrime and cyberterrorism in the global environment create new challenges for protecting the national information space. In this context, information security risk management is becoming essential for ensuring the sustainability of digital transformations and creating conditions for the sustainable development of the digital economy.

This research article aims to systematise the key aspects of information security risk management in digital transformations, in particular, to avoid risks to information systems and ensure proper protection and defence of human rights. It seeks to identify the focus of information security risks and develop modern prevention methods in the digital environment. The study provides for forming sustainable trends based on assessing the relationships between the leading indicators of digital infrastructure and cybersecurity.

LITERATURE REVIEW

Given the intensification of digital transformation processes, existing information security measures need to be more widely applied due to the growing number and intensity of information threats in those areas of social relations in which this transformation is taking place at a remarkably rapid pace Shopina [1]. According to Khaustova et al. [2], the definition of information security is based on an integrated approach. It reflects a continuous process of managing information flows of resources to increase competitiveness and ensure sustainable development of critical infrastructure and national security. Instead, Hren et al. [3] consider information security as a state of protection of the information space, a system of protection of national interests and a function of the state, which is implemented through legal and targeted actions. In this context, Bondarenko et al. [4] identified the main tasks of preventing threats in the information and communication sphere, which include, first of all, the protection of critical information infrastructure, protection of personal data, security of information and communication systems and government structures, as well as protection of the production environment and technologies.

The main measures to ensure data security in digitalisation, according to Santhi [5], include encryption, multi-level authentication, regular system updates, security audits, and data backups. The same conclusions were also reached by Dhanalakshmi and George [6], Fang [7], He et al. [8], George et al. [9], Syed et al. [10] and others. It should also be noted that, according to Horlichenko [11], the effectiveness of information security management systems is determined by the choice of measures to eliminate risks based on comparable and reproducible assessments; however, the implementation of these requirements is complicated by existing methods due to the identified limitations of their use in conditions of uncertainty.

Instead, cybersecurity, as one of the key components of information security, involves protecting critical information infrastructure, telecommunication networks, and electronic trust services from viruses, hacker attacks, and data fraud [12].

In this context, Manuilov [13] notes that the most priority ways of responding to cyberattacks include restoring the functioning of information, telecommunications and technological systems after a cyberattack, restoring information and data in case of damage or deletion, and creating the preconditions for investigating the consequences of a cyberattack. It is worth noting that studies by Ukrainian authors Bondarenko et al. [4] and Poliakov [14] revealed the lack of an effective mechanism for legal regulation of the introduction of digital innovations and electronic document management; thus, necessitating the development of regulations that provide a legal framework for the protection of electronic documents from cybercrime and fraud schemes, as well as mechanisms of liability for their violation.

In addition, some scholars also focus on data protection issues in enforcement proceedings and ensuring the observance of individual rights. Given the current problems of ensuring the proper storage and processing of personal information, Barrett [15] emphasises the critical role of the General Data Protection Regulation (GDPR), which focuses on the implementation of regulatory mechanisms that do not minimise the risks of data leakage or misuse in the course of fulfilling legal obligations, ensuring a balance between the rights of individuals and the effectiveness of law enforcement. In this context, Caruana [16] draws attention to the reform of the EU data protection system, in particular Directive 2016/680, which supports the principles of data protection in law enforcement, focusing on the delineation of its actions with the GDPR, independent supervision and regulation of international data transfers.

Other studies, such as Hanneke et al. [17], examine the GDPR through the effectiveness of the regulation in the context of its focus on a confidential approach to data protection. In particular, Atadoga et al. [18] note that the GDPR introduces data minimisation, purpose limitation, and the right to be forgotten, shaping how information is collected, processed and stored.

METHODS

The following methods were used in the research:

- The systematisation method was utilised to classify the areas of information security risks in digital transformations;
- The generalisation method was operated to identify modern tools for managing information security risks in the context of digitalisation;
- The case analysis method was employed to study the critical aspects of Ukraine's information security in the digital environment in the context of cyber warfare;
- The analysis of the regulatory framework was used to substantiate the vulnerabilities of Ukraine's current information security system;
- Statistical data analysis was conducted to identify sustainable trends in digitalisation and the development of cybersecurity measures in cyber warfare.

A paired samples T-test was used to assess statistically significant differences between the related indicators, calculated using the corresponding JASP software tool. The research criteria, i.e. related indicators, are indicators of the level of digitalisation (E-Government Development Index, Online Service Index, Telecommunication Infrastructure Index) and cybersecurity components (General cyber security indicator, Baseline cyber security indicators, Incident and crisis management indicators). The baseline data for the study is presented in Appendix B. The results of the t-test included the value of the t-statistic (t), degrees of freedom (df) and significance level (p-value), which allowed us to assess the probability of differences between the variables compared. The main limitation of the study is the small sample size (n = 3), which reduces the reliability of the results and increases the likelihood of type I (false positives) and type II (false negatives) errors.

RESULTS

Theoretical aspect of information security risk management

Given the rapid development of global digital transformations, information security is a complex and multifaceted concept that covers a set of measures to protect information from various threats that may arise during its processing, storage or transmission. Its main goal is to ensure the confidentiality, integrity and availability of information and protection against unauthorised access, modification or destruction [2]. Given the intensity of digital transformation and the constant development of technology, information security is becoming a critical element for maintaining the stability and efficiency of both individual organisations and government agencies. In this context, information systems are complex complexes that include hardware, software, databases, network resources, and organisational processes that ensure data processing and protection. As information systems continuously interact with various internal and external environments, they are exposed to numerous potential threats that may impact their operation differently. The security system must be able to respond quickly to all possible scenarios that could lead to disruption of its operation or loss of critical information. Such systems are often exposed to various types of threats that can cause various damages, which vary according to the scale and nature of the impact on information systems. The main areas of information security risks in digital transformations are shown in Figure 1.

Modern digital transformation processes have significantly impacted all areas of public life, including enforcement proceedings. On the one hand, information technologies provide new opportunities for the practical work of the enforcement officer related to the processing of large amounts of personal data; on the other hand, new challenges arise due to the growth of cyber threats and stricter requirements for the protection of information (personal data). Compliance with the requirements of the General Data Protection Regulation (the GDPR; Regulation (EU) 2016/679) is a crucial aspect of ensuring information security while enforcing court decisions and other jurisdictional bodies. Enforcers are both controllers and processors of personal data, which requires them to have a deep understanding of

the GDPR principles and the ability to apply them in practice. The author identifies several challenges related to applying the GDPR in enforcement proceedings, such as restrictions on the use of data and ensuring confidentiality and integrity of information. In order to effectively manage information security risks in the context of digital transformation, it is necessary to develop and implement comprehensive measures, including advanced training of enforcement officers, improvement of the regulatory framework and use of modern information security technologies.

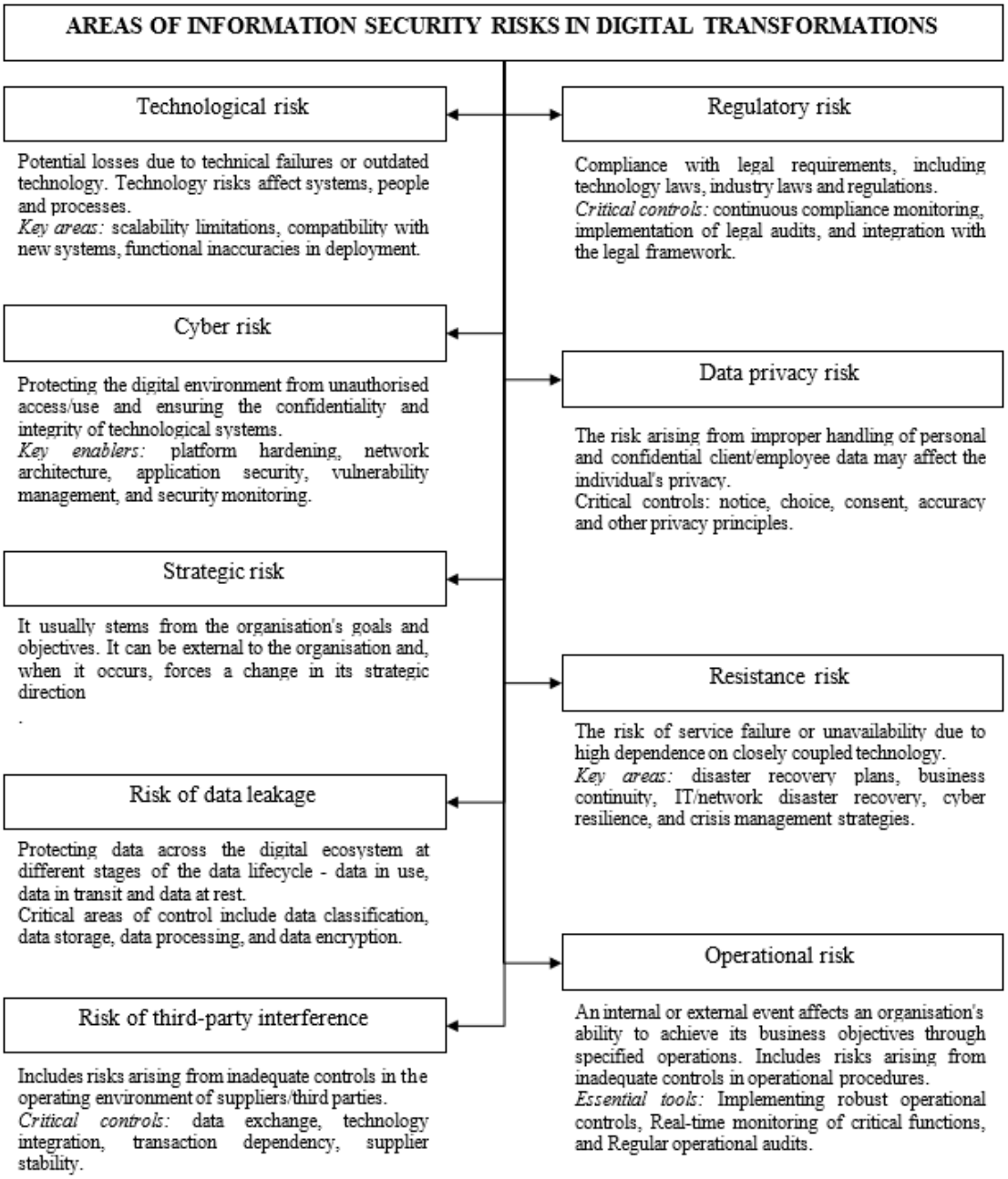

Figure 1. Characteristics of information security risk areas in digital transformations

Source: compiled by the author

In the face of increasing threats and the growing number of attacks, information security risk management is becoming a two-stage process, where the first stage is to identify and assess information security risks, and the second

involves ranking risks to develop a response strategy. Selecting the most optimal and effective methods of risk management and risk assessment is crucial, as it determines the success of information security measures [11]. Thus, the analysis of modern methods of information security risk management, shown in Figure 2, is a crucial prerequisite for developing optimal risk management strategies in the context of modern geopolitical challenges and technological threats.

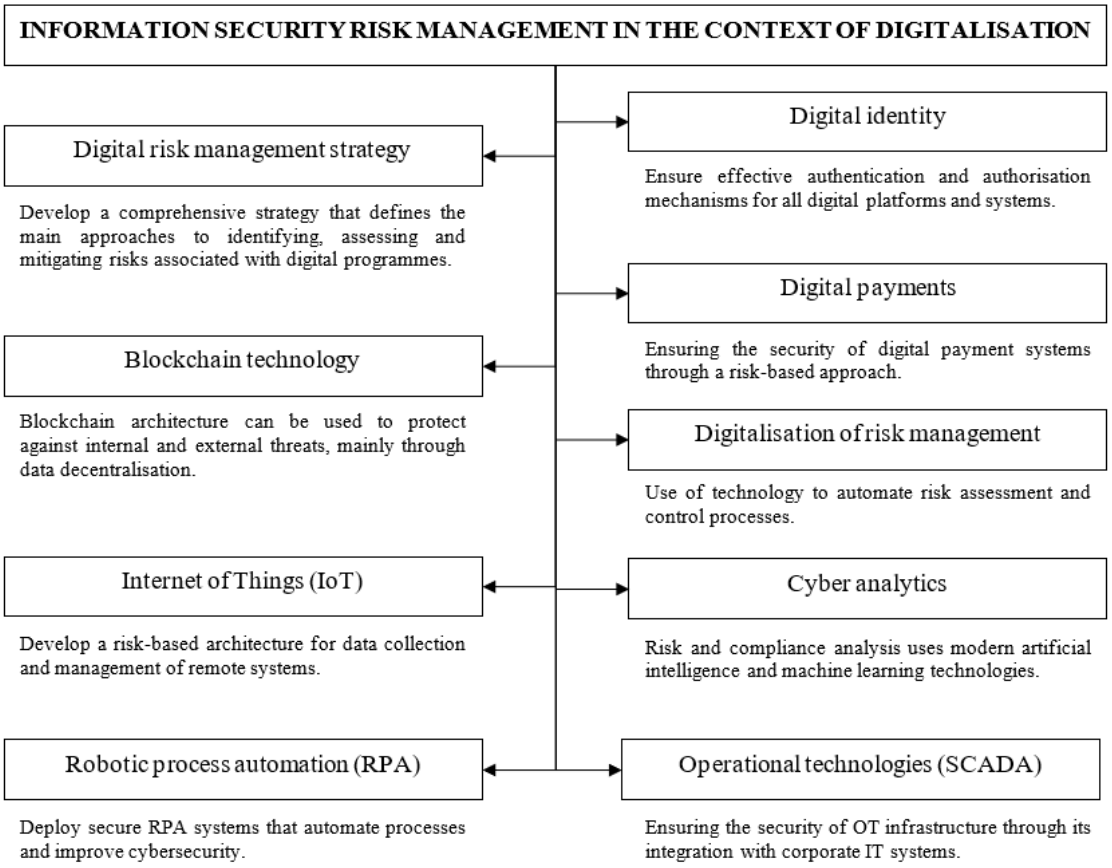

Figure 2. Information security risk management tools in the context of digitalisation

Source: compiled by the author

Thus, each of the above tools is an element of the overall system aimed at preserving the integrity, confidentiality, and availability of information systems and preventing and managing their current risks. Ensuring the effective use of these technologies helps reduce potential threats and increase the resilience of the information infrastructure to various cyber-attacks.

Information security in the digital environment in the context of cyber warfare: the case of Ukraine

Since 2014, the Russian Federation's policy towards Ukraine has been accompanied by the active use of cyber attacks to lobby for colonial interests as part of a hybrid war aimed at violating Ukraine's national security through the impact on information technology, telecommunications and critical electronic systems (document management systems, banking). The main aspects of the problem include manipulation of public opinion, political and economic pressure, and consequences for security and stability. In this context, effective counteraction to information warfare is essential for Ukraine and other countries facing Russian aggression to preserve security, stability and democratic values [12].

The first large-scale cyberattack was recorded in 2015, when Russian hackers caused a power outage in western Ukraine, one of the most prominent examples of cyber sabotage against critical infrastructure. However, the further

evolution of cyberattacks by Russia is characterised by the scale of cyber incidents, in particular the NotPetya virus attack in 2017, which had a devastating impact on financial systems, government electronic documentation and telecommunications infrastructure, confirmed Russia's strategic focus on using cyber aggression to destabilise Ukraine [19]. Among other means of cyber warfare, the most devastating were the effects of VPNFilter in 2018, which targeted Ukrainian network devices, focusing on routers and other IoT devices [20]; HermeticWiper in 2022, which aimed to destroy data in Ukrainian public and private institutions; and WhisperGate in 2022, which targeted massive data destruction in Ukrainian government agencies, banks and media companies [21].

Given the escalation of cyber warfare by Russia, the Ukrainian government has begun to develop a regulatory framework for the protection of critical information infrastructure, in particular, the adoption of the laws "On the Basic Principles of Ensuring Cybersecurity of Ukraine" and "On Critical Infrastructure" has become the basis for building an effective national cyber defence system. In this context, Ukraine's cybersecurity strategy, approved in 2021, set priorities for harmonising national legislation with international standards, strengthening coordination between government agencies and the private sector, and introducing modern technologies to counter cyber threats.

Against the backdrop of an increase in the number and scale of cyber threats, the current state cyber defence policy focuses on the development of an organisational and technical model that ensures integrated interaction of cybersecurity actors, coordination between sectors, the use of cyber analytics and the development of an incident response system. The critical aspects of ensuring information security in the context of globalisation and digital transformation, as well as against the backdrop of cyber warfare accompanied by Russia's physical aggression against Ukraine, are as follows.

Protection of critical information infrastructure

Ukraine's information infrastructure includes IT networks, data centres, servers, electronic platforms (banking, documentation), information technology and telecommunications (electronic communications), and data storage systems that ensure reliable storage and processing of information critical to all other critical infrastructure sectors.

The main threats to Ukraine's information security include the risk of targeted attacks on electronic trust services, electronic banking and document management systems aimed at stealing financial information, blocking transactions or making changes to transactions. It is worth noting that such risks are exacerbated by the dependence on foreign software vendors and the use of outdated or unlicensed technologies, leading to vulnerability to unauthorised interference. In addition, protecting public and private information systems is complicated by the imperfection of existing cyber security standards and limited capacity to respond to current information security challenges. In this context, the problem of preserving personal data and state secrets and protecting confidential information from unlawful access or transfer is a priority for ensuring the sustainability of the national information space.

Ensuring cybersecurity of information systems

Figure 3 shows the key indicators of the cybersecurity level, which combine strategic management tools, preventive measures, and mechanisms for responding to potential and current cybersecurity threats.

Figure 3. Key indicators of cybersecurity

Source: compiled by the author based on NCSI [22]

Given the need to study the mutual influence of the development of digital technologies and the overall strengthening of digital transformation on the cybersecurity of Ukrainian information systems in the context of cyber warfare, the values of the main cybersecurity indicators shown in Figure 4 were the criteria for further analysis.

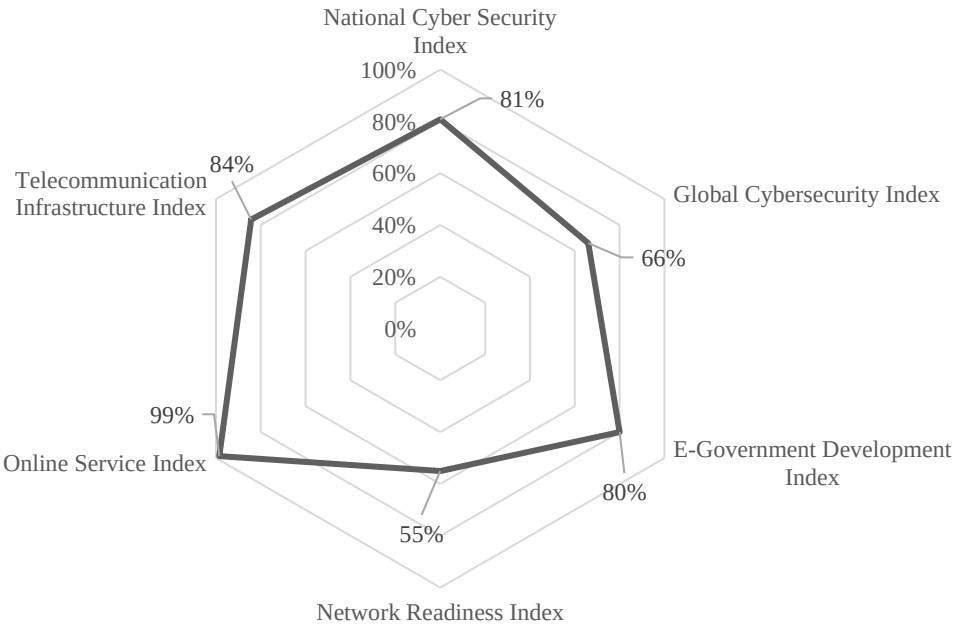

Figure 4. Rating of Ukraine's cybersecurity indicators in 2024

Source: compiled by the author based on NCSI [22]

The ranking of Ukraine's cybersecurity indicators allows us to form a modern cybersecurity profile of Ukraine. This profile is generally characterised by rapid progress in the formation of a comprehensive cybersecurity system. However, there is still a gap compared to some of the world's leading countries, which gives room for future growth in this area.

According to the NCSI [22], Ukraine currently ranks 13th (with a score of 80.83) in the global cybersecurity ranking. Although the country's cybersecurity level has shown a significant increase since 2016, from 24th place (with a score of 75.32), with the most impressive indicator of the development of electronic online services (in 2024, 5th place in the ranking), the level of digitalisation is still inferior to countries such as Estonia or Singapore, which have integrated cyber defence systems and a high level of cooperation between public and private entities. In addition to ongoing hostilities and cyberwarfare, political instability and legal and regulatory gaps are significant barriers to strengthening cybersecurity. The basis for regulatory and legal support of cybersecurity of information systems in Ukraine is provided by the Laws of Ukraine "On the Basic Principles of Cybersecurity of Ukraine", "On National Security of Ukraine", "On Critical Infrastructure"; resolutions of the Cabinet of Ministers of Ukraine "On Approval of the Regulation on the Organisational and Technical Model of Cybersecurity", "On Certain Issues of Critical Information Infrastructure Objects", "On Approval of the General Requirements for Cybersecurity of Critical Infrastructure Objects"; and the Decree of the President of Ukraine "On the Regulation on the Working Group of the National Security Council of Ukraine".

However, despite a clear regulatory framework, the lack of an integrated approach to its implementation reduces the effectiveness of protecting state electronic systems, telecommunications networks and critical information infrastructure. These challenges are in contrast to the experience of European countries (mainly due to the lack of such a sizeable cyber risk), such as the Netherlands, whose national cybersecurity strategies are aimed at clearly dividing responsibilities between sectors and thus ensuring transparency in interagency coordination. For example, the Dutch National Coordination Centre for Counter-Terrorism and Security (NCTV) coordinates the activities of various agencies, including the police, judiciary and security services. This approach generally focuses on artificial threats, developing comprehensive strategies for responding to terrorist acts and cybercrime [23].

The following criteria for assessing the relationship between the leading indicators of digital infrastructure and cybersecurity are the critical indices of Ukraine's digitalisation in 2020–2023, shown in Figure 5. The indicators of the level of digitalisation were selected in accordance with their direct impact on the state's information security.

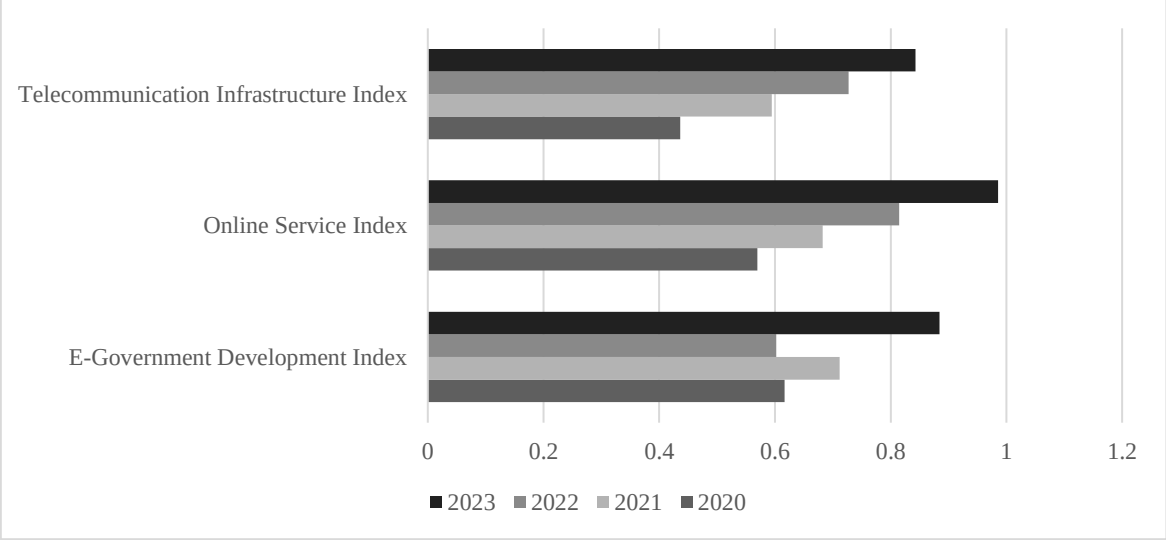

Figure 5. Trends in the development of crucial digitalisation indices in Ukraine in 2020-2023

Source: compiled by the author based on United Nations [24]

The overall level of e-government quality, as measured by the E-Government Development Index (EGDI), is currently 0.8841, showing a significant increase compared to 2020 (0.6165), which led to Ukraine's rise in the world ranking to 30th place. In turn, the Telecommunication Infrastructure Index (TII), which covers the availability and quality of telecommunications networks, has shown a steady increase in recent years to 0.8428 (30th place in the world ranking), suggesting a stable basis for the safe functioning of the digital economy and supporting the development of information security. At the same time, the government's increased efforts to ensure the availability and quality of online services, according to the Online Service Index (OSI), led to an increase in the index from 0.5694 in 2020 to 0.9854 in 2023 (5th place in the global ranking). Thus, the government's focus on introducing accessible and secure digital services strengthens citizens' trust in digital platforms and reduces the risk of confidential and personal data leakage.

To analyse the impact of digitalisation on Ukraine's information security in the context of cyber warfare, the relationships between the leading indicators of digital infrastructure and cybersecurity, the values of which are given in Appendix B, were assessed using the Paired Samples T-Test tool in the JASP software (Appendix A). The application of this method is justified by the need to identify critical dependencies between indicators of digital infrastructure development and the level of cybersecurity, which is necessary to formulate recommendations for strengthening digital resilience in information security. The results of the Paired Samples T-Test for assessing the relationships between the leading indicators of digital infrastructure and cybersecurity are presented in the Table 1.

Table 1. Results of Paired Samples T-Test to assess the relationships between key indicators of digital infrastructure and cybersecurity

Paired Samples T-Test			Measure 2								
			General cyber security indicators			Baseline cyber security indicators			Incident and crisis management indicators		
			G2	G3	G4	B1	B2	B3	I1	I2	I3
Measure 1	E-Government Development Index	t	0.614	-0.844	1.873	4.515	-1.791	-1.386	0.573	2.585	2.184
		df	3	3	3	3	3	3	3	3	3
		p	0.583	0.461	0.158	**0.020***	0.171	0.260	0.607	0.081	0.117
	Online Service Index	t	1.240	-0.352	2.505	5.266	-1.198	-0.842	1.049	4.690	2.706
		df	3	3	3	3	3	3	3	3	3
		p	0.303	0.748	0.087	**0.013***	0.317	0.462	0.371	**0.018***	0.073
	Telecommunication Infrastructure Index	t	0.314	-1.123	1.281	3.314	-2.606	-2.043	-0.133	3.587	1.758
		df	3	3	3	3	3	3	3	3	3
		p	0.774	0.343	0.290	**0.045***	0.080	0.134	0.903	**0.037***	0.177

Source: compiled by the author

Notes: G2 – Cyber threat analysis and information; G3 – Education and professional development; G4 – Contribution to global cyber security; B1 – Protection of digital services; B2 – Protection of essential services; B3 – E-identification and trust services; I1 – Cyber incidents response; I2 – Cyber crisis management; I4 – Military cyber operations.

The results of the Paired Samples T-Test revealed a number of the most statistically significant (at $p < 0.05$) aspects of the impact of digital transformation on cybersecurity:

– The statistically significant relationship between the E-Government Development Index and the Protection of Digital Services ($t = 4.515$ at $p = 0.02$) indicates an increase in the effectiveness of protecting Ukrainian digital services

at the state level by expanding e-government capabilities. In 2024, this was facilitated by the government's adoption of the Priority Areas for Digital Transformation for 2024-2026, including projects aimed at harmonising with the European Union's requirements in electronic identification and electronic trust services. Such initiatives include the modernisation of the licensing and transport registers, the creation of a Unified Register of State Property and an online lease management platform, and the integration of analytical subsystems for key government agencies [25];

– The Online Service Index has a statistically significant relationship with the Protection of digital services ($t = 5.266$ at $p = 0.013$), meaning that improved access to online services has a positive impact on the effectiveness of their protection; and Cyber crisis management ($t = 4.69$ at $p = 0.018$), meaning that increased access to online services, in particular through expanding the functionality of government portals and integrating digital registries, improves the Ukrainian government's ability to prevent the consequences of a prolonged cyber war;

– The Telecommunication Infrastructure Index has a statistically significant relationship with the Protection of digital services ($t = 3.314$ at $p = 0.045$), indicating that the impact of increased telecommunication infrastructure efficiency on improving the protection of digital services, which highlights the importance of reliable communication networks to support cybersecurity; and Cyber crisis management ($t = 3.587$ at $p = 0.037$), which highlights the ability of telecommunication networks to maintain operational resilience during a cyberwar crisis.

In addition, during the study, it is necessary to pay attention to trends that indicate the possible statistical significance of the obtained indicators (at $p < 0.10$). Therefore, the following trends were identified:

– The close to statistical significance of the relationship between the E-Government Development Index and Cyber crisis management ($t = 2.585$ at $p = 0.081$) indicates the potential impact of improving government digital services on cyber threat management;

– The correlation between Online Service Index and Contribution to global cybersecurity is close to statistical significance ($t = 2.505$ at $p = 0.087$), indicating that the growth in the quality and availability of online services may have a positive impact on the overall level of a country's cybersecurity;

– The potential relationship between the Telecommunication Infrastructure Index and the Protection of Essential Services ($t = -2.606$ at $p = 0.08$) indicates a tendency to ensure high protection of critical systems by improving telecommunications infrastructure.

Thus, positive developments in the critical areas of digitalisation contribute to strengthening cybersecurity, particularly in protecting digital and online services at the state level, ensuring the reliability of telecommunications networks, and preventing the leakage of confidential information.

DISCUSSION

Khaustova et al. [2] proved that in order to form a qualitatively new concept of critical infrastructure development from the standpoint of information security and its practical implementation, it is advisable to develop an organisational and economic mechanism, the essence of which is a set of principles, tools, functions, methods and means aimed at reducing the level of cyber risks, the cost of managing information flows and the introduction of digital technologies and software. Instead, our work focuses on cybersecurity issues, given the relevance of its provision in digital transformation and the intensification of cybercrime and cyberterrorism. In addition, our analysis revealed a statistically significant relationship between the development of e-government and the protection of digital services ($t = 4.515$, $p = 0.02$); therefore, the expansion of e-government helps to reduce the risks of digital service vulnerabilities, which is consistent with the theoretical assumptions of Shopina [1] about the need to expand information security measures due to the growing number of information threats.

The analysis of Bondarenko et al. [4] shows that the most significant mutual influence is demonstrated by the group of indicators of the institutional capacity of the state and the group of indicators of the digital capacity of the national economy and cybersecurity; this to some extent correlates with the findings of our work, which indicate the overall stability of the relationships between cybersecurity and digitalisation indicators. In turn, Horlichenko [11] notes that the effectiveness of information security management depends on the ability to assess risks and adapt to uncertainty. However, our study shows that the existing mechanisms leave room for improvement, particularly in critical information infrastructure protection.

CONCLUSION

An increase in information security risks also characterises the rapid development of digitalisation and, therefore, requires improvement of approaches to their management in the field of information systems protection, as well as protection and defence of human rights. The theoretical aspects of the study indicate the complexity and multidimensionality of the concept of information security, which includes not only technical but also organisational, legal and strategic components aimed at protecting the confidentiality, integrity and availability of information. In this context, Ukraine is a vivid example of a country that has faced large-scale information security challenges in the context of cyber warfare. The digital environment is becoming an arena for hybrid threats, including cyberattacks on critical infrastructure, spreading disinformation and manipulating public opinion through social media. Ukraine's experience demonstrates the importance of a comprehensive approach to information security based on resilience, innovation, and international cooperation as crucial elements for countering cyber threats in modern hybrid warfare.

REFERENCES

[1] Shopina, I. M. Information security of digital transformation. Scientific Bulletin of the Lviv State University of Internal Affairs (Legal Series), 2023, 1, 28–35. https://doi.org/10.32782/2311-8040/2023-1-4

[2] Khaustova, V.; Tirlea, M. R.; Dandara, L.; Trushkina, N.; Birca, I. Development of critical infrastructure from the point of view of information security. Strategic Universe Journal/Univers Strategic, 2023, 1, 170–188. https://www.ceeol.com/search/article-detail?id=1107664

[3] Hren, L.; Karpeko, N.; Kopanchuk, O.; Strelbitsky, M.; Tohobytska, V. Substantive Essence and Components of the Societal Phenomenon "Information Security" in the Age of Information Society. In: Radchenko, O.; Kovach, V.; Semenets-Orlova, I.; Zaporozhets, A. (Eds.), National Security Drivers of Ukraine. Contributions to Political Science, pp. 75–91. Springer, Cham, 2023. https://doi.org/10.1007/978-3-031-33724-6_5

[4] Bondarenko, S.; Makeieva, O.; Usachenko, O.; Veklych, V.; Arifkhodzhaieva, T.; Lernyk, S. The Legal Mechanisms for Information Security in the context of Digitalisation. Journal of Information Technology Management, 2022, 14(Special Issue: Digitalisation of Socio-Economic Processes), 25–58. https://doi.org/10.22059/jitm.2022.88868

[5] Santhi, S. K. A comparative analysis on the combined multi level functionality framework in cloud environment with enhanced data security levels for privacy preservation. Journal of Theoretical and Applied Information Technology, 2023, 101(9), 3248–3258. https://ir.vignan.ac.in/id/eprint/625/

[6] Dhanalakshmi, G.; George, G. V. S. Secure and Privacy-Preserving Storage of E-Healthcare Data in the Cloud: Advanced Data Integrity Measures and Privacy Assurance. International Journal of Engineering Trends and Technology, 2023, 71(10), 238–253. https://doi.org/10.14445/22315381/IJETT-V71I10P222

[7] Fang, F. University Data Security Practice Under the Background of Digital Transformation. In 2024 3rd International Conference on Artificial Intelligence and Computer Information Technology (AICIT), 2024, 1–4. IEEE. https://doi.org/10.1109/AICIT62434.2024.10730168

[8] He, Y.; Zhou, Z.; Pan, Y.; Chong, F.; Wu, B.; Xiao, K.; Li, H. Review of data security within energy blockchain: A comprehensive analysis of storage, management, and utilisation. High-Confidence Computing. High-Confidence Computing, 2024, 4(3), 100233. https://doi.org/10.1016/j.hcc.2024.100233

[9] George, A. S.; George, A. H.; Baskar, T. Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 2023, 1(4), 155–172. https://doi.org/10.5281/zenodo.8274514

[10] Syed, Z.; Dapaah, E.; Mapfaza, G.; Remias, T.; Mupa, M. N. Evaluating the Effectiveness of Cybersecurity Protocols in SAP System Upgrades. IRE Journals, 2024, 8(2), 129–154. https://www.irejournals.com/formatedpaper/1706115.pdf

[11] Horlichenko, S. Information security risk management methods: ISO/IEC 27001 standard and cis critical security controls. Ukrainian Scientific Journal of Information Security, 2024, 30(1), 190–196. https://doi.org/10.18372/2225-5036.30.18620

[12] Halipchak, V. Information warfare as a component of hybrid warfare in the context of Russian aggression. Bulletin of the Precarpathian University. Series: Political Science, 2023, 1(15), 26–32. https://doi.org/10.32782/2312-1815/2024-1-4

[13] Manuilov, Ya. S. Ensuring cybersecurity of critical infrastructure facilities in the context of cyberwar. Information and Law, 2023, 1(44), 154–167. https://doi.org/10.37750/2616-6798.2023.1(44).287780

[14] Poliakov, O. M. Modern trends in detecting and countering the use of spyware and malware. Information and Law, 2023, 2(45), 125–138. https://doi.org/10.37750/2616-6798.2023.2(45).282332

[15] Barrett, C. Emerging trends from the first year of EU GDPR enforcement. Scitech Lawyer, 2020, 16(3), 22–35. https://www.proquest.com/openview/1ebb532e9f48bf0f1f358412175e60a3/1?pq-origsite=gscholar&cbl=38541

[16] Caruana, M. M. The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. International Review of Law, Computers & Technology, 2019, 33(3), 249–270. https://doi.org/10.1080/13600869.2017.1370224

[17] Hanneke, B.; Baum, L.; Hinz, O. GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing. ECIS 2023 Research Papers, 2023, pp. 1–16. https://aisel.aisnet.org/ecis2023_rp/409

[18] Atadoga, A.; Farayola, O. A.; Ayinla, B. S.; Amoo, O. O.; Abrahams, T. O.; Osasona, F. A comparative review of data encryption methods in the USA and Europe. Computer Science & IT Research Journal, 2024, 5(2), 447–460. https://doi.org/10.51594/csitrj.v5i2.815

[19] Gül, Y. E. The application of the principle of precautions to cyber operations. The Military Law and the Law of War Review, 2023, 61(1), 3–38. https://doi.org/10.4337/mllwr.2023.01.01

[20] Baezner, M. Cyber and Information warfare in the Ukrainian conflict. Centre for Security Studies (CSS), 2018, 1, 1–56. https://doi.org/10.3929/ethz-b-000321570

[21] Hladka, Yu.; Halitsyn, V. Countermeasures against the use of malware as a type of cyberattacks. Science and Technology Today, 2024, 4(32), 894–908. https://doi.org/10.52058/2786-6025-2024-4(32)-894-908

[22] NCSI Fulfilment Percentage: Ukraine. National Cyber Security Index, 2024. https://ncsi.ega.ee/country/ua/

[23] Førde, J. S.; Lægreid, P.; Rubecksen, K.; Rykkja, L. H. Organising for societal security and crisis management in Germany, The Netherlands, Norway, Sweden and the UK. Societal security and crisis management: Governance Capacity and Legitimacy, 2019, pp. 27–51. https://doi.org/10.1007/978-3-319-92303-1_2

[24] United Nations. UN E-Government Survey 2024, 2024. UN E-Government Knowledgebase. https://publicadministration.un.org/egovkb/en-us/Data-Center

[25] NISD. Digital Transformation of the Ukrainian Economy in Wartime. August – September 2024. National Institute for Strategic Studies. https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-serpen-veresen

Appendix A

Groups of indicators		Name of the indicator	Period			
			2020	2021	2022	2023
Digitalisation indicators		E-Government Development Index	0,6165	0,7119	0,6023	0,8841
		Online Service Index	0,5694	0,6824	0,8148	0,9854
		Telecommunication Infrastructure Index	0,4364	0,5942	0,727	0,8428
Cybersecurity indicators	GENERAL CYBER SECURITY INDICATORS	Cyber security policy development (G1)	1	1	1	1
		Cyber threat analysis and information (G2)	0,67	0,8	0,8	0,2
		Education and professional development (G3)	0,6	0,89	0,89	0,89
		Contribution to global cyber security (G4)	1	0,33	0,33	0,33
	BASELINE CYBER SECURITY INDICATORS	Protection of digital services (B1)	0,75	0,2	0,2	0,2
		Protection of essential services (B2)	0,83	1	0,83	0,83
		E-identification and trust services (B3)	0,75	1	0,89	0,78
		Protection of personal data (B4)	1	1	1	1
	INCIDENT AND CRISIS MANAGEMENT INDICATORS	Cyber incidents response (I1)	0,64	0,67	0,67	0,67
		Cyber crisis management (I2)	0,56	0,6	0	0
		Fight against cybercrime (I3)	1	1	1	1
		Military cyber operations (I4)	1	0,17	0,17	0,17

Appendix B

Paired Samples T-Test					
Paired Samples T-Test					
Measure 1		**Measure 2**	**t**	**df**	**p**
E-Government Development Index	-	Cyber threat analysis and information	0.614	3	0.583
E-Government Development Index	-	Education and professional development	-0.844	3	0.461
E-Government Development Index	-	Contribution to global cyber security	1.873	3	0.158
E-Government Development Index	-	Protection of digital services	4.515	3	0.020
E-Government Development Index	-	Protection of essential services	-1.791	3	0.171
E-Government Development Index	-	E-identification and trust services	-1.386	3	0.260
E-Government Development Index	-	Cyber incidents response	0.573	3	0.607
E-Government Development Index	-	Cyber crisis management	2.585	3	0.081
E-Government Development Index	-	Military cyber operations	2.184	3	0.117
Online Service Index	-	Cyber threat analysis and information	1.240	3	0.303
Online Service Index	-	Education and professional development	-0.352	3	0.748
Online Service Index	-	Contribution to global cyber security	2.505	3	0.087
Online Service Index	-	Protection of digital services	5.266	3	0.013
Online Service Index	-	Protection of essential services	-1.198	3	0.317
Online Service Index	-	E-identification and trust services	-0.842	3	0.462
Online Service Index	-	Cyber incidents response	1.049	3	0.371
Online Service Index	-	Cyber crisis management	4.690	3	0.018
Online Service Index	-	Military cyber operations	2.706	3	0.073
Telecommunication Infrastructure Index	-	Cyber threat analysis and information	0.314	3	0.774
Telecommunication Infrastructure Index	-	Education and professional development	-1.123	3	0.343
Telecommunication Infrastructure Index	-	Contribution to global cyber security	1.281	3	0.290
Telecommunication Infrastructure Index	-	Protection of digital services	3.314	3	0.045
Telecommunication Infrastructure Index	-	Protection of essential services	-2.606	3	0.080
Telecommunication Infrastructure Index	-	E-identification and trust services	-2.043	3	0.134
Telecommunication Infrastructure Index	-	Cyber incidents response	-0.133	3	0.903
Telecommunication Infrastructure Index	-	Cyber crisis management	3.587	3	0.037
Telecommunication Infrastructure Index	-	Military cyber operations	1.758	3	0.177