Digital Transformation: Cybersecurity in the Age of Digitization

Sergii Bataiev [1], Leonid Maidanevych [2], Oleh Snieosikov [3], Sviatoslav Yemelianov [4], Oleksii Kharytonov [5]

[1] University of Warwick, Coventry, UK; Department of Technology, ELEKS Inc., Lviv, Ukraine.
[2] Department of Information Protection, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine.
[3] Department of Cybersecurity of Information Systems, Networks and Technologies, Educational and Research Institute of Computer Science and Artificial Intelligence, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
[4] Department of Physics and Mathematics Teaching Methods, Educational and Scientific Pedagogical Institute named after V. O. Sukhomlynsky, Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine.
[5] Interregional Academy of Personnel Management, Kyiv, Ukraine.
Corresponding author: serg.bataiev@gmail.com

© Authour(s)
OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: Relevance. Currently, the digital transformation of social, economic, and technological processes is accompanied by an exponential increase in the amount of data processed and stored in the digital environment, as well as the active implementation of automated control systems, artificial intelligence, blockchain technologies, and cloud services. Therefore, an urgent issue for the academic community, in particular for the practical implementation of information security strategies, is the study of new methods of data protection in the context of digital transformation.

Objective. The purpose of the study is to analyze the level of cybersecurity and digital readiness of the EU countries to assess the effectiveness of implemented information security strategies in the context of digital transformation.

Methods. The study uses methods of synthesizing literature sources to assess current cybersecurity trends, descriptive statistics to analyze the level of digital readiness of EU countries, and data visualization through Raincloud Plots to display the dynamics of indicators. In addition, systematization and generalization methods were used to identify effective innovative methods of data protection.

Results. The study found a positive trend towards strengthening cybersecurity and digital readiness of the EU countries, as evidenced by an increase in the average values of GCI (from 91.296 in 2023 to 93.846 in 2025) and ICTDI (from 76.259 in 2023 to 87.462 in 2025), as well as a decrease in the standard deviation of most indicators, which indicates a gradual unification of cybersecurity measures.

Conclusions. New methods of data protection will in the future contribute to the development of innovative technologies, which will strengthen the protection of information and contribute to the creation of a reliable digital environment. Therefore, the high-quality integration of innovative methods into cybersecurity strengthens data protection and contributes to the creation of a reliable digital environment for critical information systems.

Keywords: GNSS (Global Navigation Satellite System), Cybersecurity, Information and Communication System, Autonomous Differential Correction System, Satellite Navigation, GPS Spoofing, GPS Jamming, IDS (Intrusion Detection System), IPS (Intrusion Prevention System).

Introduction

In the context of digital transformations that radically change economic, social, and technological processes, cybersecurity is becoming increasingly important as the risks associated with data and information infrastructure protection scale up. The intensive introduction of large databases, blockchain technologies, digital platforms, and automated control systems contributes to the efficiency of the digital environment, while creating new threats, including cyberattacks, leakage of confidential information, and disruption of critical information systems. In this context, the dynamics of the National Cyber Security Index (NCSI) in the EU countries in 2023-2025 (Figure 1) illustrates a gradual increase in the level of national cyber resilience, which indicates the intensification of strategic measures to protect the digital space.

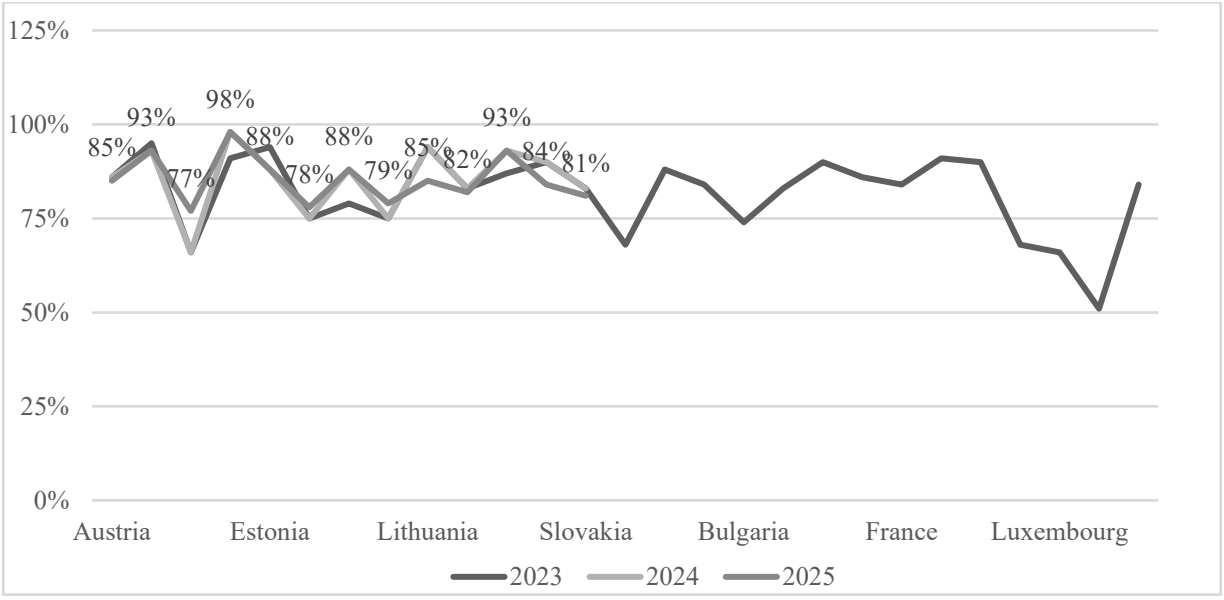


Figure 1. Dynamics of the National Cyber Security Index (NCSI) in the EU member states in 2023-2025
Source: [1]

At the same time, the escalation of cybercrime, the use of unlicensed software, and the growth of cyber threats necessitate the introduction of the latest data protection methods adapted to the rapidly changing challenges of the digital age [2]. Cybersecurity risk management is becoming a key area of ensuring the sustainability of digital transformations, which is an essential condition for the development of the modern digital economy.

The purpose of this scientific article is to comprehensively assess the level of cybersecurity and digital readiness of EU countries based on the analysis of key indicators, which allows to determine the dynamics of their development, identify the main trends and evaluate the effectiveness of implemented cybersecurity strategies in the context of digital transformation. The article is aimed at characterizing innovative methods of data protection in the context of growing cybersecurity risks and enhanced digital transformation.

Literature Review

Cybersecurity as one of the key components of information security involves the protection of critical information infrastructure, telecommunication networks and electronic trust services from viruses, hacker attacks, and data fraud [3]. In this context, Manuilov [4] notes that the most priority ways to respond 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 conducting an investigation into the consequences of a cyberattack. At the same time, Bondarenko et al. [5] and Poliakov [6] found that there is no effective mechanism for legal regulation of the introduction of digital innovations; 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. Similar conclusions were reached by Pandey and Kapoor [2], who investigated the multifaceted impact of cybercrime on vulnerable systems, causing financial,

psychological and reputational damage at various levels (governmental, social and economic). Given the current problems of ensuring the proper storage and processing of personal information, Barrett [7] emphasizes the key role of the General Data Protection Regulation (GDPR), which focuses on the implementation of regulatory mechanisms that minimize the risks of data leakage or misuse in the process of fulfilling legal obligations, ensuring a balance between the rights of individuals and the effectiveness of law enforcement. In this context, Caruana [8] 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. [9], 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. [10] note that the GDPR introduces principles such as data minimization, limitation of data processing purposes, and the right to data disposal, shaping the way information is collected, processed, and stored.

The data protection and cybersecurity landscape is evolving rapidly, driven by the need to counter increasingly sophisticated cyber threats. Santhi [11] identifies encryption, multi-level authentication, regular system updates, regular security audits, and data backups as the main measures to ensure data security in the context of digitalization. Similar conclusions were also reached by Dhanalakshmi and George [12], Fang [13], He et al. [14], George et al. [15], Syed et al. [16], and others. It should also be noted that, according to Horlichenko [17], 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. In this context, the development of new data protection methods involves the further integration of machine learning, advanced encryption, and innovative methodologies to improve data security. In particular, the DDCI uses machine learning algorithms such as anomaly detection, clustering, and predictive modeling to improve cybersecurity [18, 19]. This approach allows real-time adaptation to new threats, outperforming traditional static methods [20]. Instead, advanced Intrusion Detection Systems (IDS) incorporate sophisticated encryption algorithms and machine learning to monitor network traffic and detect anomalies; thus, providing real-time tracking and reporting, significantly reducing false alarms and increasing the accuracy of threat detection [21]. In turn, the latest cryptographic techniques, including hashing and asymmetric encryption, are needed to ensure data confidentiality and integrity [22, 23, 24]. The development of blockchain technology and post-quantum cryptography emphasizes the importance of developing cryptographic solutions to counter modern challenges [25]. Although the above-mentioned advances offer promising solutions, challenges to their implementation remain, especially in dynamic environments where threats are constantly evolving. Mainly, in the works of Ali et al. [26], Calatrava et al. [27], Polikarovskykh et al. [28], the intensification of the implementation of new data protection methods is a response to the growing cyber threats arising from the use of GPS Spoofing and GPS Jamming methods that can destabilize the functioning of global navigation satellite systems (GNSS). In this context, as noted by Xing et al. [29], the autonomous differential correction system (ADCS) deserves special attention, as it provides increased accuracy of satellite navigation signals and their resistance to interference. In Dini et al. [30], such a system is also quite applicable for an embedded system for real-time intrusion detection in automotive systems, where the synchronization problem between the CAN transceiver and ADC channels was solved by a cyclic buffer strategy that significantly reduced false alarms and increased system stability.

Methods

The following methods were used in the research process:

- synthesis of literature sources was used to analyze current trends and theoretical approaches to ensuring cybersecurity, assess the effectiveness of modern data protection mechanisms, and identify key issues in the legal regulation of the introduction of digital innovations;
- descriptive statistics of cybersecurity and digital readiness indicators of EU countries were compiled based on the official NCSI [1] reports for 2023-2025 to assess the effectiveness of the implemented digital transformation measures and their impact on the level of data protection;
- visualization was used to fully understand the current state of cybersecurity measures in the EU Member States by determining the dynamics of changes in cybersecurity indicators of the EU Member States. The process of forming visual data schemes was carried out using Raincloud Plots graphs in the JASP statistical program (Descriptives tool). The initial data was collected based on the official NCSI reporting [1] and systematized in Appendix A. The main limitation of the study is the lack of data for the analyzed period for all EU member states, which was taken into account when compiling descriptive statistics;

- the systematization method was used to identify the most effective innovative methods at each stage of security in the overall data protection system;
- the generalization method was used to justify the application of the latest data protection methods in the context of enhanced digital transformation.

Results and Discussion

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 organizations and government agencies. In this context, information systems are complex complexes that include hardware, software, databases, network resources, and organizational processes that ensure data processing and protection. Cybersecurity, as a fundamental component of overall information security, covers the protection of critical information infrastructure, telecommunication systems, and electronic trust services from threats, including viruses, unauthorized access, and data manipulation [2]. Therefore, a key vector of countering cyberattacks, which involve the prompt restoration of the functionality of information, telecommunications and technological systems, restoration of damaged or lost data, is to create conditions for investigations to identify threats and minimize their impact. Given the current landscape of data protection and cybersecurity, it is necessary to conduct a comprehensive analysis of the dynamics of key indicators of cybersecurity and digital readiness of EU member states in the period 2023-2025, which will allow assessing the effectiveness of the implemented digital transformation measures and their impact on the level of data protection. To conduct the relevant analysis, descriptive statistics of the original dataset were compiled (Appendix A), as shown in Table 1.

Table 1. Descriptive statistics of cybersecurity and digital readiness indicators of the EU countries in 2023-2025

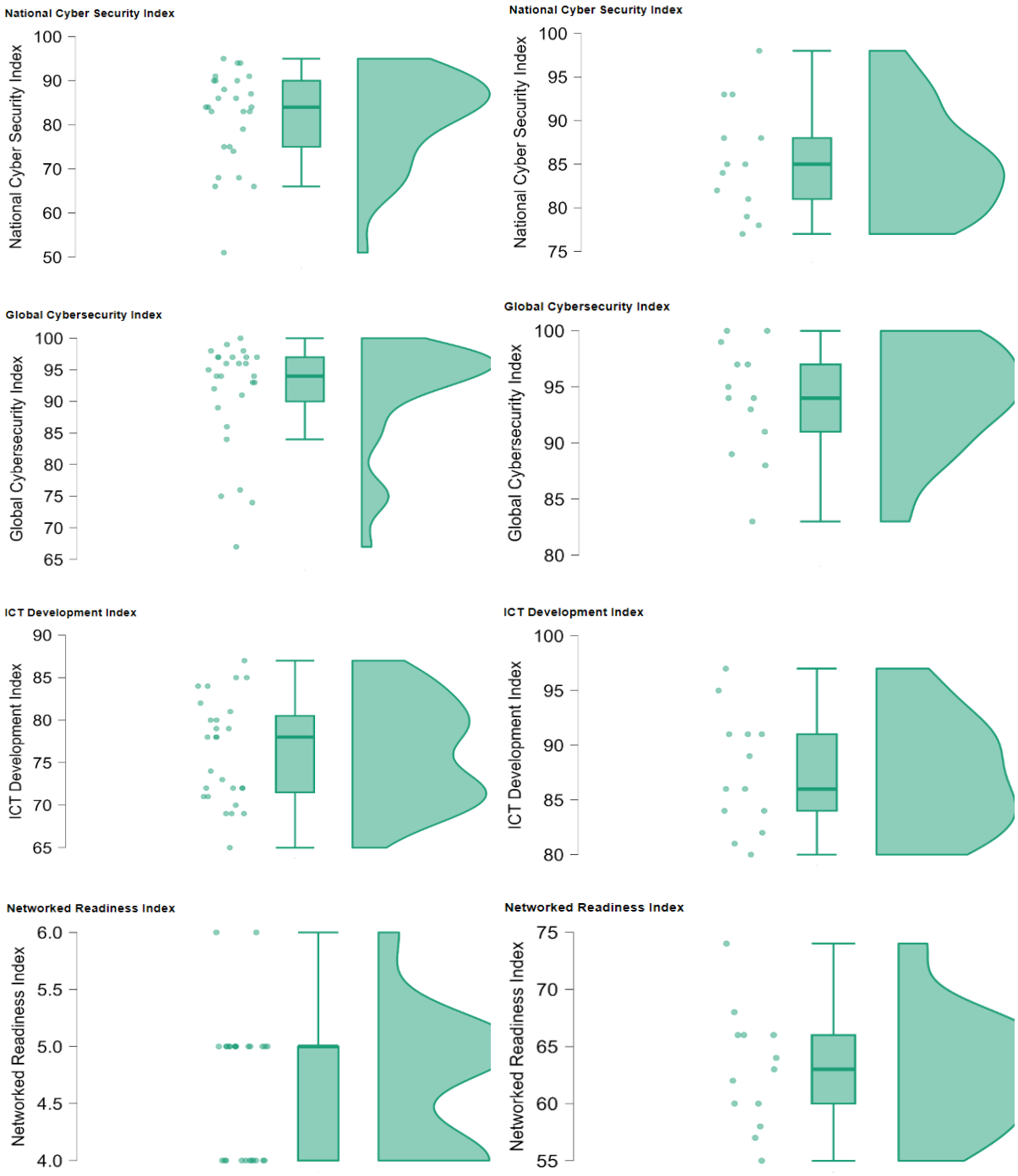
Descriptive Statistics												
Period	**2023**				**2024**				**2025**			
Indicators	NCSI	GCI	ICTDI	NRI	NCSI	GCI	ICTDI	NRI	NCSI	GCI	ICTDI	NRI
Valid	27	27	27	27	13	13	13	13	13	13	13	13
Missing	0	0	0	0	14	14	14	14	14	14	14	14
Median	84.000	94.000	78.000	5.000	88.000	95.000	80.000	5.000	85.000	94.000	86.000	63.000
Mean	81.667	91.296	76.259	4.667	85.538	94.154	80.000	27.538	85.462	93.846	87.462	63.000
Std. Deviation	10.655	8.708	6.087	0.620	9.070	4.259	7.360	30.223	6.372	5.064	5.348	5.148
Minimum	51.000	67.000	65.000	4.000	66.000	86.000	71.000	4.000	77.000	83.000	80.000	55.000
Maximum	95.000	100.000	87.000	6.000	98.000	100.000	97.000	68.000	98.000	100.000	97.000	74.000

Source: compiled by the author

Notes: NCSI – National Cyber Security Index; GCI – Global Cybersecurity Index; ICTDI – ICT Development Index; NRI – Networked Readiness Index

The analysis revealed a positive trend in the development of cybersecurity in the EU member states, which is manifested in the growth of average values of indicators, in particular the GCI and the ICT Development Index, as well as in the reduction of the variability of other indicators, which indicates the harmonization of cybersecurity policies. The most significant progress is observed in the field of digital infrastructure, as evidenced by the increase in the NRI in 2025, which indicates the effectiveness of the European Commission's strategic investments in the development of advanced cybersecurity technologies and digital transformation. However, in order to fully understand the current state of cybersecurity measures in the EU member states, it is necessary to clearly define the dynamics of changes in the cybersecurity indicators of the EU member states. To do this, based on the original data (Appendix A),

we visualized the data using Raincloud Plots in the JASP statistical program. Based on the methodology of Allen et al. [31], and combining a point cloud, box plot, and one-way violin plot, the graphs presented in Figure 2 allow for simultaneous display of the distribution, variability, and trends of predefined data.



a) Cybersecurity indicators in 2023 b) Cybersecurity indicators in 2025

Figure 2. Raincloud Plots on the dynamics of changes in cybersecurity indicators in EU member states
Source: compiled by the author

The distribution of the National Cyber Security Index (NCSI) scores shows significant variability in the level of national cybersecurity among EU member states in 2023. Although the bulk of observations are concentrated in the top quartile of the distribution, the presence of outliers indicates the presence of countries with relatively lower scores. Instead, in 2025, there is an increase in the overall level of security, as evidenced by a decrease in variance and a more concentrated location of values in the upper range, which mainly indicates the effectiveness of implemented government policies in the field of cybersecurity. Given that the identified positive developments are largely due to the strengthening of the EU's cybersecurity regulatory framework, it is worth emphasizing the fundamental importance of implementing Directive NIS 2, which expands the requirements for cyber risk management and mandatory reporting for key sectors. Additionally, the adoption of the Cybersolidarity Regulation (EU) 2025/38 laid the groundwork for a joint response to cyber threats and the creation of a European cybersecurity reserve, which provides Member States with rapid support in the event of large-scale attacks [32]. Thus, the consolidation of the regulatory environment and increased investment in cybersecurity have contributed to a more balanced distribution of security levels among EU countries.

The distribution of the Global Cybersecurity Index (GCI) shows a stable level of cybersecurity in most EU member states, although the presence of statistical outliers in 2023 may indicate an uneven distribution of cybersecurity measures among the countries studied. However, by 2025, the index values have stabilized, which is obvious given the reduction in interquartile range and the elimination of significant data anomalies. In turn, the dynamics of the ICT Development Index (IDI) reflects the progressiveness of solutions aimed at digital transformation, which is now widespread among EU member states. In 2023, there is a wide range of variations between countries, as evidenced by the wide range of distribution. This is due to the fact that the EU takes measures related to digital transformation in accordance with sectoral and horizontal policies and based on a number of provisions of the Treaty on the Functioning of the European Union (TFEU). The provisions of this Treaty are generally used as a basis for harmonization of the digital single market, in particular Articles 4(2)(a), 26, 27, 114 and 115 TFEU. In addition, Art. 173 TFEU, aimed at increasing the competitiveness of EU industry, is used to promote digital technologies, in particular in the field of confidential data protection [33]. At the same time, in 2025, the variability of IDI values is decreasing, which indicates the harmonization of the development of information and communication technologies in Europe. This is the result of the European Commission's strategic investments in five key sectors: high-performance computing, artificial intelligence, cybersecurity and trust, advanced digital skills, and ensuring the widespread use of digital technologies in the economy and society. In particular, in February 2025, the European Union announced an additional €50 billion investment in artificial intelligence, complementing the €150 billion raised from private investors under the European AI Champions initiative; bringing the total investment in this sector to €200 billion [34].

Regarding the distribution of Networked Readiness Index (NRI) values: in 2023, there was a high level of dispersion of values with a noticeable group of countries lagging behind in terms of readiness for digital transformation; and in 2025, the distribution shows a tendency to increase the average values and decrease the number of outsiders, which may indicate an overall improvement in digital infrastructure in the region. Thus, in addition to the above-mentioned increase in investment, the development of the EU's digital infrastructure was facilitated by the creation of the IRIS2 satellite network, which involves the launch of 290 satellites to provide high-speed Internet connectivity across Europe. This project, worth €10.6 billion, was officially approved in December 2024 and aims to begin operations by 2030 [35], which increases the investment attractiveness of digital infrastructure in the European space and stimulates its further development.

Thus, the analysis shows a positive trend in the development of cybersecurity in the EU member states, which is reflected in the stabilization of indicators and a decrease in the spread of values. This trend is mainly due to the effectiveness of digital transformation policies and strengthening of regulatory and legal regulation in the field of cybersecurity. In particular, increased investment in high-performance computing, artificial intelligence, and cybersecurity is currently contributing to the strengthening of digital infrastructure and the improvement of cybersecurity among member states. The above measures, which include funding research projects, developing innovative technologies, and implementing security standards, have a positive impact on stabilizing cybersecurity indicators and reducing the spread of the analyzed values.

However, despite the positive impact of current cybersecurity solutions, in today's digital transformation environment, the issue of ensuring reliable data protection is becoming critical due to the growing complexity of cyber threats, scaling of information flows, and the need to introduce innovative technologies in the field of cybersecurity. The urgency of cybersecurity, in particular in the area of data protection, is mainly due to the purpose of cyberattacks. According to the European Council of the European Union [36], almost 20% of cyberattacks are aimed at the public administration sector, which is important for the provision of public services and security, as well as at the areas of transport (11%), finance (9%), digital infrastructure (9%), business services (8%), social protection (8%) and manufacturing (6%), and the dynamics of their implementation is growing rapidly. Therefore, traditional protection methods are currently not effective enough in ensuring an adequate level of cybersecurity, which requires the use of

new approaches that combine artificial intelligence, cryptographic mechanisms, and the principles of decentralized data management (Figure 3).

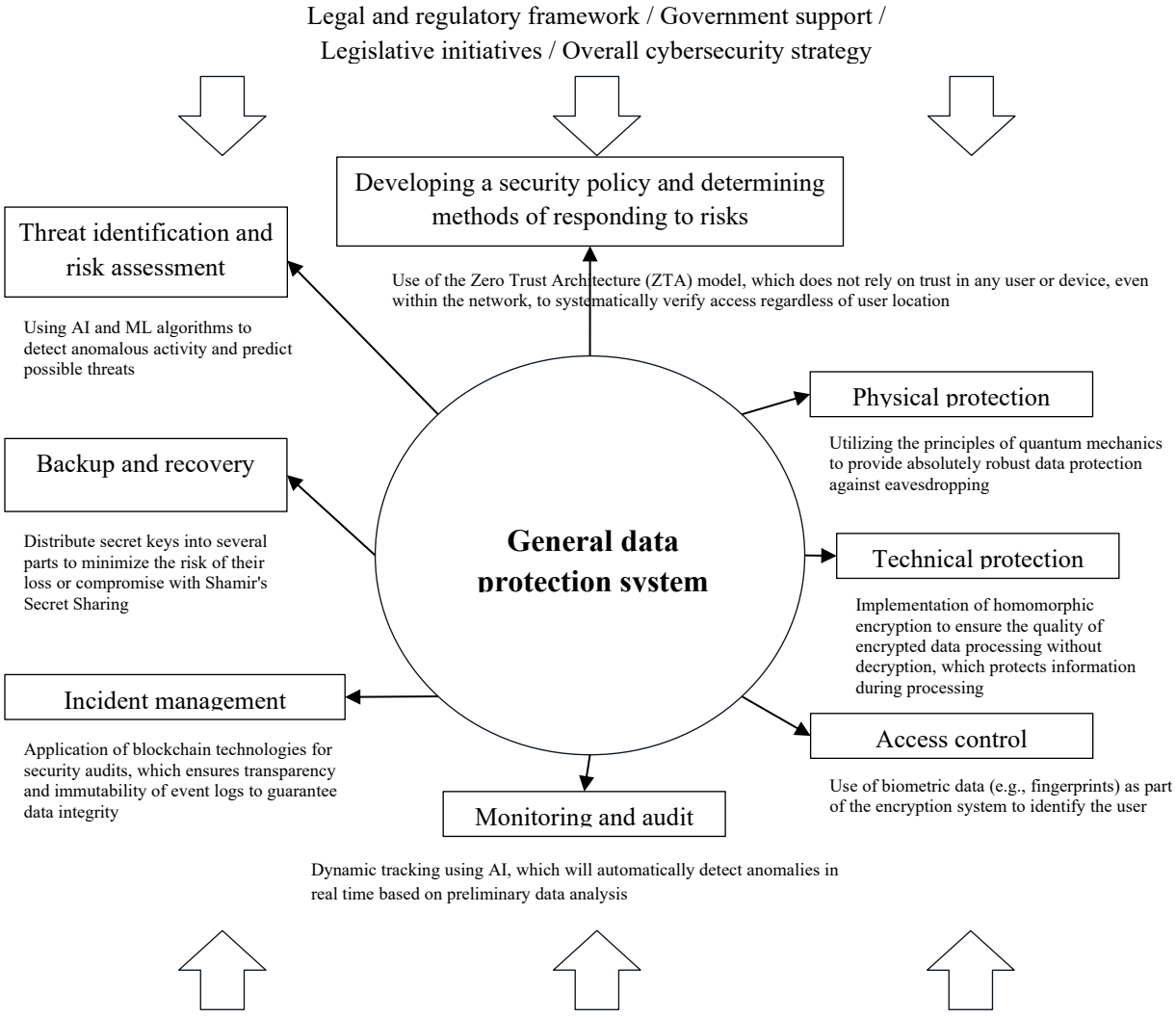


Figure 3. Application of innovative methods in the overall data protection system
Source: compiled by the author

Threat assessment and risk management require the use of artificial intelligence and machine learning methods that allow analyzing huge amounts of information, identifying abnormal patterns, and predicting potential cyber incidents [21, 37]. Such algorithms significantly reduce the level of uncertainty and allow for the implementation of proactive threat response mechanisms, which ensures effective prediction of attacks before they actually occur [18, 38]. In the process of developing security policies and identifying strategic mechanisms to counter threats, it is advisable to use the Zero Trust architecture, which fundamentally changes traditional access models by requiring constant verification of all entities in the system and excluding any default privileges [39, 40]. This approach makes it impossible for malicious intrusion into corporate networks through compromised or trusted accounts, which is a typical threat to traditional centralized systems. Instead, given the current challenges in the field of physical data protection, there is

an urgent need to use innovative approaches. The application of quantum cryptography, which uses the principles of quantum mechanics to exchange encryption keys, provides absolute protection of information from unauthorized interception, which is a revolutionary step in ensuring information security [22, 23, 24, 41]. In addition, technical data protection involves the introduction of homomorphic encryption, which, according to Liu et al. [42], Yuan et al. [37], allows you to perform calculations on encrypted data without decrypting them and, as a result, helps to maintain confidentiality in the context of remote information processing in cloud environments.

In the area of access control, biometric authentication methods combined with cryptographic technologies are becoming more widespread, which increases the level of reliability of user identification and minimizes the risk of password compromise. Control of continuous monitoring and audit of data security is made possible by the use of dynamic analysis systems based on artificial intelligence, which provide autonomous detection of suspicious actions and registration of all anomalies in real time [19, 20]. Additionally, blockchain technologies are used to ensure the transparency and immutability of security logs, which creates a trusted infrastructure for cybersecurity audits and makes it impossible to falsify records of system events [25]. Instead, incident management involves not only an effective response to cyberattacks, but also the construction of an adaptive learning system based on the analysis of previous threats and modeling of potential attack scenarios [43], which allows for the improvement of response algorithms, increasing their effectiveness in each subsequent case. The role of data backup and recovery in the overall protection system should be emphasized, where the use of Shamir's Secret Sharing ensures the distribution of secret keys among several independent nodes, which prevents their compromise [44] and guarantees the preservation of information integrity even in the event of catastrophic failures [45]. Thus, a comprehensive approach to cybersecurity that integrates innovative methods at all stages of data protection allows for a sustainable security system adapted to modern threats. In this context, the development of innovative technologies will predictably strengthen information protection and contribute to the creation of a reliable digital environment, which is a key aspect of the safe operation of critical information systems in the global cyberspace.

Conclusions

A detailed study of the dynamics of cybersecurity development in the context of digital transformation allowed for a comparative analysis of key indicators to assess the effectiveness of data protection strategies implemented in EU Member States. In addition, the considered approaches make it possible to determine the status and prospects for further development of cybersecurity measures and data protection methods in the EU Member States, as well as to predict the further development of cybersecurity measures and data protection methods in the context of global challenges related to digital transformation. The results of the study contribute to the expansion of theoretical and practical knowledge in the field of innovative data protection methods, which are critical for the future development of cybersecurity at the European level.

References

[1] NCSI (2024). NCSI Fulfilment Percentage. *National Cyber Security Index*. https://ncsi.ega.ee/country/ua/

[2] Pandey, P., & Kapoor, A. (2025). Cybercrime in the Digital Era: Impacts, Awareness, and Strategic Solutions for a Secure Future. *Sachetas*, *4*(1), 32-37. https://doi.org/10.55955/410004

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

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

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

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

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

[8] Caruana, M. M. (2019). 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, 33*(3), 249-270. https://doi.org/10.1080/13600869.2017.1370224

[9] Hanneke, B., Baum, L., & Hinz, O. (2023). GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing. *ECIS 2023 Research Papers*, 1-16. https://aisel.aisnet.org/ecis2023_rp/409

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

[11] Santhi, S. K. (2023). 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*, *101*(9), 3248-3258. https://ir.vignan.ac.in/id/eprint/625/

[12] Dhanalakshmi, G., & George, G. V. S. (2023). 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*, *71*(10), 238-253. https://doi.org/10.14445/22315381/IJETT-V71I10P222

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

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

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

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

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

[18] Gonaygunta, H., Nadella, G. S., Pawar, P. P., & Kumar, D. (2024, May). Enhancing cybersecurity: The development of a flexible deep learning model for enhanced anomaly detection. In *2024 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 79-84). IEEE. https://doi.org/10.1109/SIEDS61124.2024.10534661

[19] Hafez, A. (2024). Global Context Enhanced Anomaly Detection of Cyber Attacks via Decoupled Graph Neural Networks. *arXiv:2409.15304*. https://doi.org/10.48550/arXiv.2409.15304

[20] Singh, J. (2023). The Evolution of Cybersecurity in the Big Data Era Moving Beyond Data Protection to Data-Driven Security. *2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG)*, Indore, India, pp. 1–6. https://doi.org/10.1109/ictbig59752.2023.10456178

[21] Faris, W. F., & Mirajkar, R. (2023). Securing the Digital Perimeter Intrusion Detection for Robust Data Protection in Cybersecurity. *Research Journal of Computer Systems and Engineering, 4*(1), 84–92. https://doi.org/10.52710/rjcse.66

[22] Wamusi, R., Asiku, D., Adebo, T., Aziku, S., Simon, P. K., Zaward M., & Guma A. (2024). A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 135-169. https://doi.org/10.58496/MJAIH/2024/016

[23] Zebari, H. K., & Abduallah, W. M. A. W. M. (2025). Cryptographic Techniques for Data Privacy Preservation: A Review. *East Journal of Applied Science*, *1*(1), 40-53. https://eastpublication.com/index.php/ejas/article/view/50

[24] Zhang, G. (2024). Cryptographic Techniques in Digital Media Security: Current Practices and Future Directions. *International Journal of Advanced Computer Science & Applications*, *15*(8), 933. https://doi.org/10.14569/ijacsa.2024.0150892

[25] Adeyinka, K. I., & Adeyinka, T. I. (2024). Cybersecurity Measures for Protecting Data. *Advances in Information Security, Privacy, and Ethics Book Series*, 365–414. https://doi.org/10.4018/979-8-3693-9491-5.ch016

[26] Ali, Z., Su, C. L., Terriche, Y., Rouhani, S. H., Hoang, L. Q. N., Sadiq, M., ... & Elsisi, M. (2025). Cyber resilience in shipboard microgrids: adaptive hybrid artificial intelligent methods and systematic review. *Neural Computing and Applications*, 1-42. https://doi.org/10.1007/s00521-025-11090-z

[27] Calatrava, H., Tang, S., & Closas, P. (2025). Advances in Anti-Deception Jamming Strategies for Radar Systems: A Survey. *arXiv preprint arXiv:2503.00285*. https://doi.org/10.48550/arXiv.2503.00285

[28] Polikarovskykh, O., Malaksiano, M., Piterska, V., Daus, Y., & Tkachenko, M. (2025). Measures to Counter Cyber Attacks on Maritime Transportation. In *Maritime Systems, Transport and Logistics I: Safety and Efficiency of Operation* (pp. 197-212). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-82027-4_13

[29] Xing, W., Li, M., Li, M., & Han, M. (2025). Towards Robust and Secure Embodied AI: A Survey on Vulnerabilities and Attacks. *arXiv:2502.13175*. https://doi.org/10.48550/arXiv.2502.13175

[30] Dini, P., Zappavigna, M., Soldaini, E., & Saponara, S. (2025). Embedded Machine Learning-based Voltage Fingerprinting for Automotive Cybersecurity. *IEEE Access, 13*, 38342-38367. https://doi.org/10.1109/ACCESS.2025.3545245

[31] Allen, M., Poggiali, D., Whitaker, K., Marshall, T. R., van Langen, J., & Kievit, R. A. (2021). Raincloud plots: A multi-platform tool for robust data visualization [version 2; peer review: 2 approved]. *Wellcome Open Research, 4*(63), 1-52. https://doi.org/10.12688/wellcomeopenres.15191.2

[32] NIS2 (2025). The NIS 2 Directive. https://www.nis-2-directive.com/

[33] EUR-Lex (2012). Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union*, 47-326. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

[34] Chee, F. Y. (2025). EU's AI push to get 50 billion euro boost, says von der Leyen. *Reuters*. https://www.reuters.com/technology/artificial-intelligence/eus-ai-push-get-50-bln-euro-boost-eus-von-der-leyen-says-2025-02-11/?utm_source=chatgpt.com

[35] Hollinger, P. (2024). Europe signs €10.6bn Iris² satellite deal in bid to rival Elon Musk's Starlink. *The Financial Times LTD*. https://www.ft.com/content/8e75ed31-0c72-4160-b406-1ca6aa36a84f?utm_source=chatgpt.com

[36] European Council of the European Union (2025). What are the top cyber threats in the EU?. *The official website of the Council of the EU and the European Council*. https://www.consilium.europa.eu/en/policies/top-cyber-threats/#:~:text=Nearly%2020%25%20of%20cyberattacks%20target,and%20manufacturing%20(6%25)%20sectors

[37] Yuan, J., Liu, W., Shi, J., & Li, Q. (2025). Approximate homomorphic encryption based privacy-preserving machine learning: a survey. *Artificial Intelligence Review*, *58*(3), 82. https://doi.org/10.1007/s10462-024-11076-8

[38] Bielialov, T., Kalina, I., Goi, V., Kravchenko, O., & Shyshpanova, N. (2023). Global experience of digitalization of economic processes in the context of transformation. *Journal of Law and Sustainable Development, 11*(3), art. no. e0814.

[39] Abid, N. (2024). Advancements and Best Practices in Data Loss Prevention: A Comprehensive Review. *Global Journal of Universal Studies*, *1*(1), 190-225. https://www.neliti.com/publications/590136/advancements-and-best-practices-in-data-loss-prevention-a-comprehensive-review#cite

[40] Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. *TechRxiv*. https://doi.org/10.36227/techrxiv.173933211.18231232/v1

[41] Klochan, V., Piliaiev, I., Sydorenko, T., Khomutenko, V., Solomko, A., & Tkachuk, A. (2021). Digital platforms as a tool for the transformation of strategic consulting in public administration. *Journal of Information Technology Management, 13*, 42-61. https://doi.org/10.22059/JITM.2021.80736

[42] Liu, W., You, L., Shao, Y., Shen, X., Hu, G., Shi, J., & Gao, S. (2025). From accuracy to approximation: A survey on approximate homomorphic encryption and its applications. *Computer Science Review*, *55*, 100689. https://doi.org/10.1016/j.cosrev.2024.100689

[43] Ahmadi-Assalemi, G., Al-Khateeb, H., Benson, V., Adamyk, B., & Ammi, M. (2025). Adaptive learning anomaly detection and classification model for cyber and physical threats in industrial control systems. *IET Cyber-Physical Systems: Theory & Applications*, *10*(1), e70004. https://doi.org/10.1049/cps2.70004

[44] Cheon, J. H., Cho, W., & Kim, J. (2025). Improved Universal Thresholdizer from Iterative Shamir Secret Sharing. *Journal of Cryptology*, *38*(1), 15. https://doi.org/10.1007/s00145-024-09536-z

[45] Iwamura, K., & Kamal, A. A. A. M. (2025). Secure User Authentication with Information Theoretic Security using Secret Sharing Based Secure Computation. *IEEE Access*, *13*, 9015-9031. https://doi.org/10.1109/ACCESS.2025.3526632

Appendix A

Country	National Cyber Security Index (NCSI)			Global Cybersecurity Index (GCI)			ICT Development Index (ICTDI)			Networked Readiness Index (NRI)		
	2023	2024	2025	2023	2024	2025	2023	2024	2025	2023	2024	2025
Austria	86%	86%	85%	94%	94%	89%	80%	80%	91%	5%	5%	66%
Belgium	95%	93%	93%	96%	97%	97%	78%	81%	81%	5%	66%	66%
Bulgaria	74%	-	-	67%	-	-	69%	-	-	4%	-	-
Croatia	83%	-	-	93%	-	-	72%	-	-	4%	-	-
Cyprus	66%	66%	77%	89%	89%	97%	78%	78%	86%	4%	4%	57%
Czech Republic	91%	98%	98%	74%	88%	88%	72%	82%	82%	5%	63%	63%
Denmark	84%	-	-	93%	-	-	87%	-	-	5%	-	-
Estonia	94%	88%	88%	100%	95%	95%	81%	97%	97%	5%	68%	68%
Finland	86%	-	-	96%	-	-	79%	-	-	5%	-	-
France	84%	-	-	98%	-	-	82%	-	-	5%	-	-
Germany	91%	-	-	97%	-	-	84%	-	-	5%	-	-
Greece	90%	-	-	94%	-	-	72%	-	-	4%	-	-
Hungary	68%	-	-	91%	-	-	69%	-	-	4%	-	-
Ireland	75%	75%	78%	86%	86%	91%	80%	80%	91%	5%	5%	66%
Italy	79%	88%	88%	96%	100%	100%	70%	84%	84%	4%	64%	64%
Latvia	75%	75%	79%	97%	97%	83%	73%	73%	89%	4%	4%	58%
Lithuania	94%	94%	85%	98%	98%	93%	72%	72%	91%	4%	4%	60%
Luxembourg	66%	-	-	97%	-	-	85%	-	-	5%	-	-
Malta	51%	-	-	84%	-	-	79%	-	-	5%	-	-
Netherlands	83%	83%	82%	97%	97%	99%	85%	85%	95%	6%	6%	74%
Poland	87%	93%	93%	94%	94%	94%	69%	86%	86%	4%	60%	60%
Portugal	90%	90%	84%	97%	97%	100%	71%	71%	84%	5%	5%	62%
Romania	90%	-	-	76%	-	-	65%	-	-	4%	-	-
Slovakia	83%	83%	81%	92%	92%	94%	71%	71%	80%	4%	4%	55%
Slovenia	68%	-	-	75%	-	-	74%	-	-	5%	-	-
Spain	88%	-	-	99%	-	-	78%	-	-	5%	-	-
Sweden	84%	-	-	95%	-	-	84%	-	-	6%	-	-