# Cybersecurity as a factor of national and European security: the experience of Slovakia in the EU context[1]

Olena Plaksiuk[1,†], Oksana Yakusheva [2,†], Oleksandr Yakushev[3,†], Oleksandr Chernyshov[4,†]

[1] *Dmytro Motornyi Tavria State Agrotechnological University, 18 B.Khmelnytsky Ave, Melitopol, Zaporizhzhia obl.72312, Ukraine*

[2] *Cherkasy State Technological University, Shevchenka, 460, 18000, Cherkasy, Ukraine*

[3] *Cherkasy State Technological University, Shevchenka, 460, 18000, Cherkasy, Ukraine*

[4] *State University "Kyiv Aviation Institute", 1, Liubomyra Huzara ave. Kyiv, 03058 Ukraine*

**Abstract**

The publication highlights the issue of the state of cybersecurity in the Slovak Republic and the EU. The essence and relationship of cybersecurity with information security are revealed, successful examples of the implementation of cybersecurity projects in the Slovak Republic and the EU are presented. Based on the NCSI index, the readiness of EU countries and Slovakia in particular to prevent cyber threats and manage cyber incidents is determined.

**Keywords**

cybersecurity, financing, management, European Union, Slovak Republic.

## 1. Introduction

Cybersecurity is a set of processes, best practices, and technology solutions that help protect critical systems and networks from digital attacks. As the volume of data grows and more people work and connect to the network from anywhere, attackers respond by developing sophisticated methods to gain access to resources and steal data, sabotage businesses, countries, or extort money. The number of attacks increases every year, and attackers develop new methods to avoid detection. An effective cybersecurity program includes people, processes, and technology solutions that together reduce the risk of business loss, financial loss, and reputational damage resulting from an attack.

At the same time, cybersecurity is a state in which networks and information systems are able to withstand, with a reasonable degree of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of data stored, transmitted, or processed, or of related services provided or accessed through those networks and information systems. [1,2]

The main purpose of the publication is to identify and analyze current trends related to cybersecurity, to generalize theoretical approaches and practical experience of European Union countries to combine theory with applied practice in implementing relevant cybersecurity projects.

## 2. Results

Information security is part of the security management of the entire organization. It involves working with information in general and includes the so-called computer security at the IT technology level. Information security differs from cybersecurity in scope and purpose.

[1] *SMICS'25: Workshop on Cryptology and Data Security, October 16-18, 2025, Lviv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

plaksyk4@gmail.com (O. Plaksiuk); o.yakusheva14@gmail.com (O. Yakusheva); aleksandro@i.ua (O. Yakushev); s.chernishov@i.ua (O. Chernyshov)

0000-0002-8707-9350 (O. Plaksiuk); 0000-0002-4849-0323 (O. Yakusheva); 0000-0002-0699-1795(O. Yakushev); 0000-0003-0422-2252 (O. Chernyshov)

These two terms are often used interchangeably, but, more precisely, cybersecurity is a subcategory of information security. In cyberspace, a multitude of threats arise every day, which often develop into real attacks.
Although these threats and vulnerabilities have different nature and form, and their calculation is practically impossible, in practice it is necessary to highlight those threats that in the medium term need to be responded to in a timely and adequate manner. [3-5]

The new Cybersecurity Regulation, which lays down measures to ensure a high common level of cybersecurity in the institutions, bodies, offices and agencies of the European Union, entered into force on 7 January 2024. The new legal framework is based on the Commission's proposal for a cybersecurity regulation of March 2022 and the political agreement reached by the European Parliament and the Council in June 2023. The comprehensive measures of the Regulation to achieve a high level of cybersecurity underline the importance of establishing an internal cybersecurity governance, management and control system that is adapted to the needs of each EU entity and takes into account the evolving nature of cyber threats and the interconnectedness of digital systems.

The Regulation establishes an Interinstitutional Cybersecurity Board to oversee and facilitate the implementation of the Regulation, ensuring that the Union institutions work towards a common cybersecurity standard. The Regulation expands the Computer Emergency Response Team for the EU Institutions (CERT-EU) to serve as a central hub for threat intelligence, information exchange and incident response coordination – it has been renamed the Cybersecurity Service for the Union Institutions, while keeping the acronym CERT-EU. [7,8]

In July 2020, the Commission published a Communication on the EU Security Union Strategy for 2020-2025. The main actions set out therein include “common rules on information security and cybersecurity for all EU institutions, bodies and agencies”. This new structure aims to foster close and effective cooperation, with CERT-EU playing a central role. In its Cybersecurity Strategy for the Digital Decade[6,14], published in December 2020, the Commission committed to presenting a proposal for a Regulation on common rules on cybersecurity for all EU institutions, bodies and agencies. It also proposed creating a new legal basis for CERT-EU to strengthen its mandate and funding. [3]

The European Parliament has approved the financing of the new Digital Europe Programme in the amount of 9.2 billion euros for 2021-2027. As reported on the European Parliament website, the aim of the programme is to strengthen the EU's competitiveness in the field of cybersecurity and in such innovative areas as supercomputers, big data processing, artificial intelligence, etc. The programme envisages financing projects for the development of digital skills and e-governance (including the implementation of "smart cities" systems and the digitalisation of healthcare, education, justice, etc.).

This Programme is part of a strategy to further develop the Digital Single Market, which could help create four million jobs and boost the EU economy with an annual budget of €415 billion each year, while increasing the EU's international competitiveness. The Digital Europe Programme allocates funds to areas such as building supercomputers (€2.7 billion), research into artificial intelligence (€2.5 billion), strengthening the EU's cybersecurity capacity (€2 billion), promoting the widespread use of digital technologies (€1.3 billion) and developing digital skills (€7 billion). [9]

There are already successful examples of cybersecurity projects under the Digital Europe Programme that are already changing people’s lives. The European Digital Media Observatory (EDMO) is the EU’s largest interdisciplinary network for countering disinformation. Its aim is to combat online disinformation that threatens democracy in the EU. EDMO is made up of 14 national and multinational centres: it is managed by a consortium led by the European University Institute in Florence, Italy. The consortium includes Athens Technology Center from Greece, Aahrus University from Denmark and the fact-checking organisation Pagella Politica from Italy. The network brings together fact-checkers working on the EDMO digital platform, media literacy experts and academic researchers to understand and analyse disinformation, as well as media organisations and media literacy professionals. Within the framework of the Digital Europe program, EDMO attracted EU co-financing of 30 million euros.

EU Digital Identity Wallet Pilots is a personal digital wallet that will allow a person to securely identify themselves when accessing a number of public and private services. The project is implemented by 2 lead countries (France, Germany) and 18 partner countries (Austria, Belgium,

Cyprus, Czech Republic, Estonia, Finland, Greece, Hungary, Italy, Latvia, Luxembourg, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Ukraine). The aim of the EU Digital Identity Wallet Pilots project is to create a single and secure digital identity system that will allow EU citizens to securely and conveniently identify themselves in the online environment, access public and private services, and increase the level of trust in digital services. The total amount of funding is 46 million euros.

Jupiter: The First European Exascale Supercomputer. Jupiter will be the first European exascale supercomputer, providing a huge boost to the EU AI ecosystem and supporting the development of high-precision models of complex systems and applications. This project aims to create a supercomputer capable of performing calculations with exascale performance, i.e. up to 10^18 (one billion billion) floating-point operations per second. The project is co-funded by EUR 250 million.

Quite interesting in the field of cybersecurity is the CyberSecPro project, which trains IT professionals to overcome current and future cybersecurity challenges. 15 higher education institutions and 13 security companies are involved in the development of a flexible, collaborative and multimodal curriculum. The project bridges the gap between science and industry, transforming theoretical knowledge into practical skills. CyberSecPro partners will develop tools to develop advanced cybersecurity skills, as well as certificates for students and professionals. CyberSecPro experts have already identified cybersecurity skills gaps in Europe and conducted a series of short training events. The project is currently developing best practice training models for cybersecurity training programmes that meet industry requirements. CyberSecPro co-funding is €6.7 million. [10]

The EU reaffirms its commitment to the peaceful resolution of international disputes in cyberspace, including through diplomatic and legal instruments. The 2015 EU Council Conclusions on Cyber Diplomacy state that the same norms and principles that the EU recognises offline, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms, should also apply in cyberspace. They also stress that the EU should actively promote a free and open internet, improve cooperation in the fight against cybercrime and strengthen cyber capacity in third countries, and call for closer cooperation between all stakeholders on cybersecurity.

At EU level, a European Cybersecurity Policy is currently being prepared to strengthen preparedness against cyberattacks, as well as a new European Cyberresilience Law, which aims to unify common standards for digital products and value-added services as a basic prerequisite for strengthening the resilience of European cyber systems and processes to cyberattacks. In response to the current situation in Ukraine, during which attacks on state facilities and telecommunications systems were also recorded, the EU activated the Cyber Rapid Response Team (CRRT) for the first time at the request of Ukraine. [11]

The National Cybersecurity Index (NCSI) has been developed to analyze and assess countries' readiness to prevent cyber threats and manage cyber incidents. [12] The NCSI is also a database of publicly available materials and tools for building national cybersecurity capacity. An overview of the European Union countries that rank highest among the world's countries according to the NCSI index is shown in Table 1.

**Table 1**

Ranking of European Union countries according to the NCSI 2025

| Rank | Країна | National Cyber Security Index | Digital Development Level |
|---|---|---|---|
| 1 | Czech Republic | 98,33 | 72,93 |
| 2 | Estonia | 96,67 | 78,14 |
| 3 | Finland | 95,83 | 85,76 |
| 4 | Romania | 92,50 | 64,57 |
| 5 | Poland | 92,50 | 73,21 |
| 6 | Belgium | 92,50 | 73,55 |
| 7 | Germany | 90,83 | 75,73 |

| | | | |
|---|---|---|---|
| 8 | France | 89,17 | 78,08 |
| 9 | Denmark | 89,17 | 85,59 |
| 10 | Italy | 88,33 | 73,58 |
| 11 | Lithuania | 85,00 | 75,53 |
| 12 | Austria | 85,00 | 78,35 |
| 13 | Portugal | 84,17 | 72,94 |
| 14 | Croatia | 82,50 | 70,07 |
| 15 | Netherlands | 81,67 | 84,66 |
| 16 | Bulgaria | 80,83 | 67,30 |
| 17 | Slovakia | 80,83 | 67,55 |
| 18 | Latvia | 79,17 | 73,10 |
| 19 | Switzerland | 79,17 | 81,88 |
| 20 | Ireland | 77,50 | 78,89 |

The NCSI is developed and implemented by the Estonian e-Government Academy Foundation, while the Global Cybersecurity Index (GCI)2 is compiled by the International Telecommunication Union (ITU), a stakeholder initiative aimed at raising awareness of cybersecurity and measuring countries' commitment to cybersecurity and its widespread application across industries and sectors. The level of development of each country is analyzed in five categories: legal measures, technical measures, organizational measures, capacity building, and cooperation. [13]

As we can see from the table, the first place in the ranking among EU countries is occupied by the Czech Republic. Slovakia, although a country very close mentally and territorially, occupies only 17th place among EU countries and 24th place in the world. The ranking of countries by NCSI is graphically depicted in Figure 1. [13]


**Figure 1:** Ranking of the Slovak and Czech Republics for the National Cybersecurity Index 2025. [13]

In 2016, the Slovak government responded to the dynamic development in the field of information and communication technologies and the growth of security threats and risks in cyberspace by strengthening the competences of the National Security Office of the Slovak Republic (NSO) in the field of coordination of activities to ensure the cybersecurity of the state at the national level. In the same year, the Slovak government approved the independent statute of the National Security Office

of the Slovak Republic, which granted it competences in the field of cybersecurity. These processes were defined in the Act on Cybersecurity, approved in January 2018, which, among other things, states that the National Security Office of the Slovak Republic, in cooperation with the Ministry of Diplomacy, develops international cooperation in the field of cybersecurity.

The program statement of the Government of the Slovak Republic for 2020-2024 draws attention to the need to strengthen protection against cyberattacks and identifies cybercrime as one of the most dangerous social challenges. The Security Strategy of the Slovak Republic (2021) emphasizes that cyberspace security is extremely important for the proper functioning and sustainability of the state and our society. The Security Strategy also draws attention to the intensification of global competition for technological and strategic advantage in cyberspace. In January 2021, the Government of the Slovak Republic approved the National Cybersecurity Strategy for 2021-2025, which sets the direction of the development of the Slovak Republic in this area and whose vision is to strengthen an open and secure cyberspace. The National Strategy is based on the Action Plan for the Implementation of the National Cybersecurity Strategy for 2021-2025, which defines specific tasks related to individual activities, responsible persons, and time horizons. [11]

## 3. Conclusion

The study confirmed that within the framework of information security, cybersecurity is the most risky due to its rapidly changing and progressive aspects, international dimension and existence in different systems. The biggest threats are misuse and theft of data, breaches of systems storing personal data, phishing attacks, but most importantly, in many aspects, the absence or insufficiency of standards, laws, regulations and insufficient awareness. In the context of comparing cybersecurity in the EU and the Slovak Republic, it can be said that the EU establishes and implements solutions for managing cybersecurity mainly within the framework of regulations and the creation of other organizations and councils to combat cyber threats, which also requires significant financial resources.

However, achieving adequate resilience to cyber threats has become one of the main priorities of the European Union in recent years. Many measures introduced by the European Union are also followed by the Slovak Republic. Cybersecurity in the Slovak Republic is addressed by a complex system that includes not only the laws regulating it, but also practical activities such as risk management, detection and resolution of cyber incidents, system recovery, education, dissemination of security information and, last but not least, research and development of cybersecurity tools and processes.

## Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT to: translate certain text fragments into English, perform grammar and spelling checks, and paraphrase or reword content. After using these tools, the authors carefully reviewed and edited the content as needed and take full responsibility for the publication's content.

## References


[1] Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts. URL: https://static.slov-lex.sk/static/SK/ZZ/2018/69/vyhlasene_znenie.html

[2] Hutsaliuk O., Bondar Iu., Kalinin O., Sokolovskiy V., Navolokina A. Integration Development of Logistics Activities of Corporate Enterprises Based on Intellectualization and Management Technologies. Intelligent Transport Systems: Ecology, Safety, Quality, Comfort. ITSESQC 2024. Lecture Notes in Networks and Systems. Cham: Springer, 2025. 1335. 270-289. URL: https://doi.org/10.1007/978-3-031-87376-8_24

[3] European court of auditors. 2022. Special Report - Cybersecurity of EU institutions, bodies and agencies: the overall level of preparedness does not match the threats. Luxembourg: Publications Office of the European Union, 2022. vol. 05. p. 62. ISBN 978-92-847-7599-6

[4] Hutsaliuk O., Havrylova N., Alibekova B., Rakayeva A., Bondar Iu., Kovalenko Yu. Management of Renewable Resources in the Energy Sector: Environmental, Economic and Financial Aspects. Green Energy and Technology. Circular Economy for Renewable Energy. Cham: Springer, 2023. 69-89. URL: https://doi.org/10.1007/978-3-031-30800-0

[5] Hutsaliuk O., Bondar Iu., Tomareva-Patlahova V., Kalinin O., Navolokina A., Kozlovska S. Integration of Operational and Economic Security of the Enterprise: Reorganization, Technologies, Risks and Outsourcing. Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies. Cham: Springer, 2025. 240. 35-61. URL: https://doi.org/10.1007/978-3-031-81557-7_3

[6] National security office. 2021. National Cyber Security Strategy for 2021 to 2025. URL: https://www.nbu.gov.sk/narodna-strategia-kybernetickej-bezpecnosti/

[7] Microsoft. 2024. What is Cybersecurity?. In: Security 101. 2024. URL: https://www.microsoft.com/enus/security/business/security-101/what-is-cybersecurity

[8] Pingen, A. 2023. New Regulation for Cybersecurity of EU Institutions. In: Eucrim.eu 2023. vol. 4. URL: https://eucrim.eu/news/new-regulation-for-cybersecurity-of-eu-institutions/

[9] European Parliament to finance new EU competitiveness program in cybersecurity. URL: https://eu-ua.kmu.gov.ua/news/yevroparlament-profinansuye-novu-programu-konkurentospromozhnosti-yes-u-sferi-kiberbezpeky/

[10] Successful projects of the EU Digital Europe Programme. URL: https://business.diia.gov.ua/history-of-success/uspishni-proiekty-prohramy-yes-tsyfrova-yevropa

[11] Ministerstvo zahraničných vecí a európskych záležitostí slovenskej republiky. 2022. Kybernetická bezpečnosť. URL:https://www.mzv.sk/diplomacia/bezpecnostnapolitika/kyberneticka-bezpecnost

[12] NCSI Project Team. e-Governance Academy. URL: https://ncsi.ega.ee/contact/

[13] Liliya Oleksiuk. Best practices in cybersecurity management. 2018. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/Report_on_Cybersecurity_04.pdf

[14] European Parliament (EP). 2022. How the Parliament wants to boost cybersecurity in the EU . URL: https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vk0gkfd9vbfw