COLLABORATION BETWEEN EU MEMBER STATES TO DEVELOP CYBER SECURITY

CZU: 004.056:061.1EU
DOI: https://doi.org/10.53486/csc2025.15

CAPAȚINA VALENTINA
Academy of Economic Studies of Moldova
valentina@ase.md
ORCID ID: 0009-0007-9767-7243

STAVENSCHI INGA
University Alexandru Ioan Cuza, Faculty of Law, Iasi, Romania
stavenschi.inga@gmail.com

Abstract: Over time, technological advancements have brought significant opportunities across various fields but have also generated challenges, including the rise of cyberattacks. In an increasingly digitalized world, cybersecurity has become a top priority for individuals, public institutions, and private organizations. Cyber threats such as ransomware attacks, phishing, and data breaches can have severe consequences on critical infrastructure, the economy, and personal privacy.

The European Union and its member states are making continuous efforts to reduce vulnerabilities in IT systems by developing comprehensive cybersecurity strategies. A key example is the NIS Directive (Network and Information Security), which imposes strict measures for securing networks and information systems.

The importance of cybersecurity became even more evident during the COVID-19 pandemic when online activities significantly increased, leading to a higher risk of cyberattacks. In response, the EU adopted a recovery plan that includes substantial investments in data protection and digital infrastructure. These measures aim to safeguard privacy, enhance trust in the digital environment, and develop more secure cyber systems across Europe.

Keywords: Cybersecurity, digital security, European Union, data protection, cyber-attacks.

JEL Classification: O33

INTRODUCTION

Cybersecurity is a particularly important area, designed to protect systems and networks against unauthorized access, theft and damage of data. Accelerated digitization and the constant interconnection of systems make technology indispensable in everyday life, influencing both professional and personal environments. The role of cybersecurity is colossal in preventing the disruption or hijacking of essential services, ensuring that digital infrastructures function properly. Most studies in this area focus on questions such as: How can EU Member States work together more effectively to prevent and combat cyber attacks? Or what policies and regulations are most effective to improve cybersecurity in the European Union.

The aim of this paper is to analyze the cooperation mechanisms between EU Member States to prevent and combat cyber threats.

The objectives pursued in this research:

- to identify the main challenges and solutions at European level;
- to identify legislative policies initiated by the EU;

- identifying collaborative initiatives and strategies implemented by Germany, France and Romania.

BASIC CONTENT

Analysis of bibliographical sources: In order to carry out this research we consulted the strategies and institutions of the European Union in order to analyze the importance of cybersecurity for the states. The main sources used were European legislation and reports carried out on the subject. Each of these sources helped us in our proposed approach, namely to analyze the challenges that states are currently facing in terms of cybersecurity.

Description of the research method used: At the basis of this paper is an analytical research with the aim of gaining an overview of digital infrastructure and its protection.

The European Union has adopted several measures to strengthen cybersecurity, including the EU Cybersecurity Strategy and the NIS (Network and Information Security) Directive, later replaced by NIS2. These initiatives aim to strengthen national capabilities, improve information sharing and create a single legislative framework for all Member States (BSI. *German Cybersecurity Strategy Report*, 10). The European Union Agency for Cyber Security (ENISA) also plays a key role in coordinating action at European level. ENISA supports Member States by developing guidelines and best practices, organizing security exercises and facilitating the exchange of information between national authorities. The recently established European Cyber Security Competence Center in Bucharest also contributes to research and development of innovative solutions to protect against digital threats (ENISA. *European Union Agency for Cybersecurity Annual Report*, 25). Moreover, incident reporting mechanisms such as the CERT-EU (Computer Emergency Response Team for the EU Institutions) platform help to monitor and manage risks in real time (CERT-EU. *Cybersecurity Threat Landscape Report*, 9).

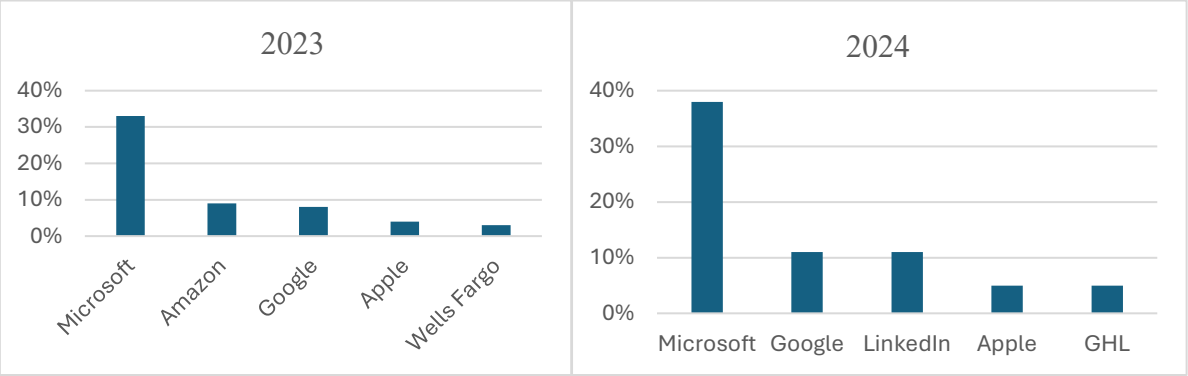

Figure 1. Top companies with cyber attacks 2023-2024.

Sourcer: *Author based on data https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf/*

According to the data presented in Figure 1, Microsoft remains the most spoofed brand in phishing attacks demonstrating the importance of its digital services in European organizations, including public institutions. In this respect, the EU, through the NIS2 Directive, imposes strict measures for the protection of critical digital infrastructures, including mandatory reporting of cyber-attacks and the implementation of enhanced security standards among public institutions and large companies. On the other hand, the emergence of LinkedIn as one of the top spoofed brands shows that cyber attacks are no longer just targeting email accounts or financial services, but also professional networks. This trend is worrying, as it may affect both the European digital economy

and the security of companies operating in the EU market (CSIRT Network. *EU Computer Security Incident Response Teams Cooperation Framework*, 5).

Cybersecurity is thus becoming a strategic priority for the European Union, essential to protect its digital infrastructure. The EU has adopted directives and regulations to increase cyber resilience and coordinate response to threats. The NIS Directive, adopted in 2016 and updated through NIS2 in 2022, imposes strict security measures for critical infrastructure and improves information sharing between Member States. NIS2 expands its scope to include more critical sectors and strict risk management requirements (European Data Protection Board. *Guidelines on Data Protection*, 17). The Cybersecurity Regulation in 2019 strengthened ENISA's role by giving it extended powers and introducing a certification framework for IT products and services (ENISA, 20). GDPR also indirectly contributes to cybersecurity by imposing strict standards for data protection and incident notification (*Guidelines on Data Protection*, 6). International cooperation plays a key role, with the EU working with NATO, the US and other organizations to exchange information and common cyber defense strategies (European External Action Service, 2).

The European Union has developed several mechanisms to strengthen cybersecurity and manage cross-border incidents. The Cyber Crisis Liaison Organization Liaison Network (CyCLONe) facilitates the coordination of response to major attacks, and the CSIRT Network brings together national teams for information exchange and mutual support. For technological development and training of specialists, the EU has set up the EU Cybersecurity Competence Network, while the NATO-supported Cooperative Cyber Defence Centre of Excellence (CCDCOE) offers training programs and attack simulations (*Cyber Diplomacy and International Cooperation*, 5). National strategies vary between Member States, with Germany emphasizing critical infrastructure protection and collaboration with the private sector through institutions such as BSI and Cyber Security Council Germany. France, on the other hand, prioritizes digital sovereignty and the protection of national infrastructures through ANSSI, taking a more restrictive approach towards foreign technologies (*International Cybersecurity Policy Analysis*, 14). Romania has strengthened its cybersecurity through national strategies and alignment with EU legislation. The adoption of NIS2 through GEO 155/2024 has extended the scope of protective measures and the DNSC has taken over the role of CERT-RO as the single point of contact for cyber incidents. (ENISA Threat Landscape, 18)

Romania also actively participates in Cyber Europe, the exercises organized by ENISA, and cooperates with Europol in the fight against cybercrime (*Cybersecurity and Risk Management*, 22). Funded through Horizon Europe and Digital Europe, the country is investing in cyber infrastructures and services. Germany therefore emphasizes critical infrastructure protection and collaboration with the private sector, France prioritizes digital sovereignty and strictly regulates the use of foreign technologies, and Romania has strengthened its strategy by aligning with EU directives and developing European partnerships. Despite these differences, a common factor remains the need for cross-border cooperation and the implementation of proactive measures to combat cyber attacks (*Octopus: Cybercrime and Electronic Evidence*, 24).

CONCLUSIONS

In an era of rapidly advancing digitization, cybersecurity is becoming an essential pillar of the economic and social stability of the European Union. The continuous evolution of cyber threats, from ransomware attacks to phishing frauds and data breaches, requires close cooperation between Member States and constant adaptation of the legislative and operational framework.

Romania, as an integral part of this security ecosystem, has made significant progress through the transposition of the NIS2 Directive and active participation in European initiatives. The establishment of the European Cyber Security Competence Centre in Bucharest is a recognition of the country's contribution in this field and provides opportunities for research, innovation and funding for the development of advanced cyber protection solutions. At the same time, Romania's involvement in European security exercises, such as Cyber Europe organized by ENISA, demonstrates its commitment to strengthen its operational capabilities in the face of emerging cyber risks.

The study of cybersecurity in the European context is essential for understanding how digital policies influence economic and social stability.

The novelty of this research lies in the comparative analysis of legislative mechanisms and their impact on economic entities, but also in highlighting Romania's role as an emerging cybersecurity hub.

The originality of the study lies in identifying the main challenges and opportunities for international cooperation in the field of digital security. Although the current analysis provides a broad perspective on the EU legislative framework and initiatives in cybersecurity, there are certain limitations. One of the main obstacles is the lack of up-to-date data on the actual effectiveness of adopted policies. Future studies could address the impact of regulations on SMEs and the public sector, as well as assess the effectiveness of strategies to prevent cyber attacks.

BIBLIOGRAPHY

1. BSI. *German Cybersecurity Strategy Report*. 2023. Bundesamt für Sicherheit in der Informationstechnik, https://bsi.bund. Accesat 2 martie 2025.
2. CCDCOE. *Cyber Defence Research and Training*. 2023. NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org. Accesat 2 martie 2025.
3. CERT-EU. *Cybersecurity Threat Landscape Report*. 2023. Computer Emergency Response Team for the EU, https://cert.europa.eu. Accesat 2 martie 2025.
4. CSIRT Network. *EU Computer Security Incident Response Teams Cooperation Framework*. 2023, https://www.csirt.eu. Accesat 2 martie 2025.
5. ENISA. *European Union Agency for Cybersecurity Annual Report*. 2023. European Union Agency for Cybersecurity, https://www.enisa.europa.eu. Accesat 2 martie 2025.
6. European Commission. *The EU's Cybersecurity Strategy for the Digital Decade*. 2022, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy. Accesat 2 martie 2025.
7. European Data Protection Board. *Guidelines on Data Protection*. 2023, https://edpb.europa.eu. Accesat 2 martie 2025.
8. European External Action Service. *Cyber Diplomacy and International Cooperation*. 2023, https://eeas.europa.eu. Accesat 2 martie 2025.
9. "ENISA Threat Landscape 2024."*European Union Agency for Cybersecurity*, 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Accesat 2 martie 2025.
10. Grecu Partners. *Cybersecurity and Risk Management*. https://grecupartners.ro/. Accesat 2 martie 2025.
11. Sciendo. *International Cybersecurity Policy Analysis*. https://intapi.sciendo.com. Accesat 2 martie 2025.
12. Council of Europe. *Octopus: Cybercrime and Electronic Evidence*. https://www.coe.int/en/web/octopus. Accesat 2 martie 2025.