DOI: http://doi.org/10.31617/1.2026(167)08
UDC 004.056:061.1ЄС=111

SHKUROPADSKA Diana
https://orcid.org/0000-0002-6883-711X
PhD (Economics),
Associate Professor at the Department
of Economics and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
diana.shkuropadska2016@knute.edu.ua

LEBEDEVA Larysa
https://orcid.org/0000-0001-8632-5460
PhD (Economics), Associate Professor,
Associate Professor at the Department of Economics
and Competition Policy
State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
l.lebedeva@knute.edu.ua

DIGITAL RESILIENCE AND CYBERSECURITY OF EU COUNTRIES

The increasing frequency and complexity of cyber threats, combined with systemic digital disruptions, have made cybersecurity and digital resilience critical determinants of the stable functioning of socio-economic systems in the European Union. The research hypothesis assumes that a country's digital resilience is shaped by real cyber incidents in combination with institutional capacity, technological readiness, and the ability to restore digital systems. To test the hypothesis, a comparative analysis combined with statistical analysis methods was applied. Cybersecurity is assessed using the Global Cybersecurity Index and the Cyber-dependent Crimes Index. Adaptive resilience potential was measured using the European Digital Resilience Index (EDRIX), complemented by the European Open Technology Readiness Index (EOTRIX). The results show that, in a theoretical aspect, cybersecurity and digital resilience are complementary: cybersecurity is a necessary functional component that provides protection against cyberattacks and unauthorized interference, while digital resilience has broader functions, including crisis management, post-incident recovery, and adaptation to new threats. The analysis of the proposed indicators within the EU

ШКУРОПАДСЬКА Діана
https://orcid.org/0000-0002-6883-711X
доктор філософії, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна
diana.shkuropadska2016@knute.edu.ua

ЛЕБЕДЕВА Лариса
https://orcid.org/0000-0001-8632-5460
к. е. н., доцент, доцент кафедри економічної
теорії та конкурентної політики
Державного торговельно-економічного
університету
вул. Кіото, 19, м. Київ, 02156, Україна
l.lebedeva@knute.edu.ua

ЦИФРОВА СТІЙКІСТЬ ТА КІБЕРБЕЗПЕКА КРАЇН ЄС

Зростаюча частота та комплексність кіберзагроз у поєднанні з системними цифровими збоями зробили кібербезпеку та цифрову стійкість критичними детермінантами стабільного функціонування соціально-економічних систем у Європейському Союзі. Гіпотеза дослідження передбачає, що цифрова стійкість країни формується реальними кіберінцидентами в поєднанні з інституційним потенціалом, технологічною готовністю та здатністю відновлювати цифрові системи. Для перевірки гіпотези застосовано порівняльний аналіз у поєднанні з методами статистичного аналізу. Кібербезпека оцінюється за допомогою Глобального індексу кібербезпеки та Індексу кіберзалежних злочинів. Адаптивний потенціал стійкості вимірювався за допомогою Європейського індексу цифрової стійкості (EDRIX), доповненого Європейським індексом готовності до відкритих технологій (EOTRIX). Результати показують, що в теоретичному аспекті кібербезпека та цифрова стійкість доповнюють одна одну: кібербезпека є необхідним функціональним компонентом, який забезпечує захист від кібератак і несанкціонованого втручання, тоді як цифрова стійкість має ширші функції, зокрема управління кризами, відновлення після інцидентів та адаптацію до

revealed the absence of a direct linear relationship between cybersecurity levels and cybercrime, as well as between cybersecurity and digital resilience. Greece, Malta and Cyprus demonstrate a high level of cybersecurity but a relatively low level of digital resilience. In contrast, Germany, Finland, Estonia, and Slovenia, are characterized by both high digital resilience and cybersecurity, indicating that digital resilience is indeed formed under the pressure of increasing threats in conditions where institutions are prepared to respond to them adequately, promptly, and systematically, which confirms the article hypothesis.

Keywords: digital resilience, cybersecurity, digitalization, crisis phenomena, European Union.

нових загроз. Аналіз запропонованих індикаторів у межах ЄС виявив відсутність прямого лінійного зв'язку між рівнями кібербезпеки та кіберзлочинністю, а також між кібербезпекою та цифровою стійкістю. Греція, Мальта та Кіпр демонструють високий рівень кібербезпеки, але порівняно низький рівень цифрової стійкості. Натомість Німеччина, Фінляндія, Естонія та Словенія характеризуються високими як цифровою стійкістю, так і кібербезпекою, що свідчить про те, що цифрова стійкість дійсно формується під тиском наростаючих загроз в умовах, коли інститути готові адекватно, оперативно й системно на них реагувати, що підтверджує гіпотезу статті.

Ключові слова: цифрова стійкість, кібербезпека, цифровізація, кризові явища, Європейський Союз.

JEL Classification: O33, L86, H56, F52.

Introduction

Digitalization has now become a global trend and a key driver of economic development, which simultaneously increases the vulnerability of countries around the world to cyber threats. Cyber incidents, failures of information systems, attacks on critical infrastructure and the spread of cyber-related crimes are increasingly becoming systemic and are capable of causing large-scale economic, social and institutional consequences. In these conditions, ensuring digital resilience is gaining strategic importance, as it involves not only protecting digital systems, but also their ability to function continuously, adapt to threats and recover from crisis impacts. Therefore, studying the relationship between digital resilience and cybersecurity is important for developing effective approaches to managing digital risks and ensuring the long-term stability of modern socio-economic systems. This issue is particularly relevant for EU countries that are forming a common digital space and seeking to ensure a high level of reliability and security of digital environments within the framework of integration processes. Increasing cross-border interaction, growing interdependence of digital infrastructures and the complexity of cyber threats necessitate a systematic scientific analysis of the state of digital resilience and cybersecurity of EU Member States. Research on this topic is important for identifying existing imbalances, assessing the level of readiness to digital risks and justifying directions for improving the security and resilience of the EU's digital development.

Under current geopolitical conditions, digital transformation has ceased to be a purely technological process, evolving into a fundamental cornerstone of national security and economic stability. For the European Union, which strives to achieve "digital sovereignty", the protection of the information space has evolved from the concept of "cybersecurity" (viewed as a set of technical protective measures) to the broader notion of "digital

resilience". The latter is understood not only a system's ability to withstand attacks but also as the capacity of critical infrastructure to maintain vital functions during incidents and recover swiftly thereafter.

The modern discourse on the European Union's security architecture is increasingly cantered on digital resilience. The transition from reactive cybersecurity to proactive resilience is most evident in the EU's recent legislative changes. The European Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA) represent a paradigm shift. The CRA introduces mandatory cybersecurity requirements for products with digital elements, thus institutionalizing a "duty of care" for manufacturers. T. Alcalá (2025), emphasizes that this legislation shifts the burden of security from the end-user to the developer as the CRA ensures that security is not an afterthought but is integrated into the entire lifecycle of digital products, from design to decommissioning.

Research into the Cyber Resilience Act (European Commission, 2025, December) highlights a paradigm shift toward "security-by-design". Kerttunen (2024) analyses how mandatory cybersecurity requirements for hardware and software products create a horizontal legal framework that reduces vulnerabilities across the EU supply chain.

The ENISA Threat Landscape (2025) highlights the "convergence of malicious activity," where threat groups increasingly use AI to automate and industrialize attacks. Recent literature suggests that the EU's resilience will depend on the rapid adoption of AI-driven defence mechanisms to counter harmful generative AI exploits (WEF, 2025)

In the financial sector, as analysed by Biliavskyi et al. (2024) digital transformation integrate digital technologies into all areas of business making it more effective. Industry reports, particularly the KPMG Cybersecurity Considerations 2025, highlight the dual nature of emerging technologies. AI Trust has become a central pillar of digital resilience. KPMG notes that CEOs see cybersecurity as the biggest threat to business in the past decade. With the rapid digitalization of all industries, particularly amid the massive adoption of AI, not only are companies' infrastructures at risk, but also their reputations, customer relationships, and even the markets they operate in (KPMG, 2025).

Academic studies by Carrapico & Farrand (2024) link these technical measures to the broader concept of "Digital Sovereignty." The research argues that resilience is no longer just a technical metric but a geopolitical tool used by the EU to ensure its autonomy in a fractured global digital world. In terms of policy, this means that it has transitioned into a system of stringent regulatory oversight and hierarchical governance, aimed not only at the internal consolidation of its cyberspace but also at projecting European security norms as global benchmarks through strategic foreign policy initiatives.

Further studies highlight digital resilience as a result of close public-private collaboration and enhanced effectiveness of public policy digital infrastructure. It is stressed that, in the context of rising hybrid threats, Europe's security depends on strong public–private partnerships and

supportive conditions for digital companies to grow in Europe (Digital Europe, 2023, March 6). Rotar (2025) emphasizes the integration of cybersecurity and resilience in national digital policies, showing that institutional and regulatory measures enhance digital governance and regional comparability. Sorokina et al. (2024) identifies the key digital determinants of national economic resilience highlighting the role of digital infrastructure, policy frameworks, and strategic digital transformation measures in strengthening the resilience of national economies facing external shocks and structural challenges.

Bada and Agrafiotis (2021) emphasize the growing "cyber inequity" and skills gap. They argue that while large organizations show steady progress, smaller organizations struggle to maintain resilience, with the public sector facing a 49% deficit in necessary cybersecurity talent as of 2025.

Contemporary research often treats cybersecurity and digital resilience as synonymous terms within the EU's strategic discourse. However, a significant gap exists in understanding the potential trade-offs and synergies between these two concepts. This study addresses this oversight by evaluating the level of cybersecurity versus resilience performance, identifying whether standardized security measures are sufficient for crisis-era functionality or if a distinct set of resilience-oriented metrics is required to sustain the EU's digital ecosystem.

The authors of the article propose *the hypothesis* that a country's digital resilience is shaped by actual cyber incidents in combination with institutional capacity, technological readiness, and the ability to restore digital systems.

The aim of the study is to evaluate the levels of cybersecurity and digital resilience in EU member states, and determine the empirical interrelationship of cybersecurity and digital resilience within the context of digital systems' capacity to neutralize crisis events and maintain functionnality.

To achieve this goal, *methods* of comparative cross-national analysis with statistical analysis were used. Specifically, to evaluate the defensive potential of EU nations, the Cybersecurity Index (GCI) was used to measure legal, technical, and organizational maturity. This was correlated with the Cyber-dependent Crimes Index to assess the actual prevalence of threats and the effectiveness of existing countermeasures. Next, to measure the adaptive capacity of systems, the European Digital Resilience Index (EDRI) was applied, that describes the ability of national infrastructures to withstand systemic shocks. This was complemented by the European Open Technology Readiness Index, that evaluates the technological flexibility and openness of the digital ecosystem.

Finally, the comparison analysis was used to determine the strength of the link between a country's cybersecurity and its resilience performance. By comparing these indices, the authors identify the cases where a high cybersecurity does not necessarily lead to high resilience and vice versa.

The structure of the article is organized as follows. First, the theoretical foundations of digital resilience and cybersecurity are analysed. Next, the level of cybersecurity within the EU's digital environment is assessed using the Global Cybersecurity Index and the Cyber-dependent

Crimes Index. This is followed by an evaluation of the digital resilience levels of EU member states, utilizing the European Digital Resilience Index and the European Open Technology Readiness Index. Finally, the study concludes with a summary of findings.

1. Theoretical understanding of digital resilience and cybersecurity

The theoretical foundations of digital resilience and cybersecurity are being formed in the context of the rapid digitalization of economy, public administration and other social processes, that causes the growing dependence of the functioning of modern systems on information and communication technologies. Under such conditions, any disruptions in the operation of digital systems caused by cyberattacks, technical failures, the human factor or hybrid threats can have large-scale economic, social and security consequences. This highlights the need for a theoretical conceptualization of cybersecurity and digital resilience, their content, interrelationship, and role in ensuring the stability of modern socio-economic systems.

Cybersecurity is a set of measures aimed at protecting information in computer systems and networks from unauthorized access, use, disclosure, violation of integrity, modification or destruction. It encompasses technical, organizational, legal, and institutional mechanisms designed to ensure the confidentiality, integrity, and availability of information resources. Cybersecurity has become vital both for protecting users' private data and personal information and for ensuring the smooth operation of critical systems, including financial institutions, government information resources, energy networks, and medical facilities. Cybersecurity breaches in these areas can lead not only to economic losses but also to threats to national security and public life. Historically, the explosion of interest in cybersecurity occurred at the end of the 20th and beginning of the 21st centuries in connection with the emergence of the Internet and the widespread use of computer technology. The further growth in the number and complexity of cyberattacks, development of malicious software, as well as the active use of digital technologies in all spheres of society contributed to the transformation of cybersecurity into a separate field of scientific knowledge and professional activity. Within this field, risk-oriented, institutional and socio-technical approaches have been formed, which consider cybersecurity not only as a set of technical solutions, but as a comprehensive cyber risk management system. At the same time, the further evolution of the digital environment has revealed the limitations of the classical understanding of cybersecurity, focused mainly on preventing threats. In response, the concept of digital resilience was formed, which originates from the general theory of systems, the economics of sustainable development, the theory of risks and crisis management. Digital resilience is interpreted as the ability of digital systems, organizations and institutions to anticipate potential threats, withstand negative impacts, adapt to changes and quickly restore their functioning after incidents, regardless of their origin.

The distinctive features of the concepts of "digital resilience" and "cybersecurity" are given in *Table 1*.

Table 1

Distinctive features of the concepts of "Digital resilience" and "Cybersecurity"

Criterion	Digital resilience	Cybersecurity
Essence of the concept	The ability of digital systems to anticipate, withstand, adapt to, and recover from disruptions and attacks	A system of measures aimed at preventing, detecting, and neutralizing cyber threats
Purpose	Continuity of operations and recovery	Protection against unauthorized interference
Time horizon	Before, during, and after an incident	Mainly before and during an incident
Scope	A broader concept (includes cybersecurity)	A narrower concept (a component of digital resilience)
Objects of impact	IT systems, business processes, human capital, institutions	Data, networks, software
Outcome	System flexibility and adaptability	System security/protection

Source: developed by the authors.

Unlike cybersecurity, digital resilience has a broader meaning and focuses not only on protecting information and infrastructure, but also on ensuring the continuity of business and management processes, maintaining the functional capacity of systems in crisis conditions and their long-term adaptability. It assumes the availability of redundant resources, backup channels, flexible organizational structures, as well as the ability to learn from experienced crises. Thus, digital resilience reflects the transition from the logic of "absolute protection" to the logic of "system viability" in conditions of constant instability. In the European Commission's approach, digital resilience and cybersecurity are considered as interrelated and complementary components of a single EU digital policy aimed at ensuring the stable, secure and continuous functioning of the digital economy and society. The European Commission considers that the modern digital environment is characterised by a high level of interdependence, cross-border threats and the constant evolution of cyber-attacks, which makes it impossible to reduce security solely to the technical protection of information systems (European Commission, 2020). In this context, cybersecurity is interpreted by the European Commission as a key element of protecting networks, information systems and data from unauthorised access, misuse and cyber-attacks, especially in critical infrastructure sectors. The Commission stresses that effective cybersecurity is a necessary prerequisite for trust in digital technologies, the functioning of the EU internal market and the protection of citizens' fundamental rights (European Commission, n. d.). That is why, within the framework of the European digital strategy, a set of legislative initiatives was formed aimed at unifying requirements for cyber risk management, strengthening the role of national authorities and coordinating the actions of member states, in particular through the adoption of the NIS2 directive and

the development of pan-European mechanisms for responding to cyber incidents (European Commission, 2022, December 14).

At the same time, the European Commission is consistently expanding the scope of the security discourse, integrating the concept of digital resilience into it. Digital resilience is understood as the ability of digital systems, organizations and economic sectors not only to withstand cyberattacks, but also to maintain operational capacity in crisis conditions, recover quickly from incidents and adapt to new types of threats (European Commission, 2025, December). This approach reflects the evolution from the classical understanding of security to a systemic concept of the viability of digital ecosystems, which is consistent with modern scientific approaches to risk management and the resilience of complex systems (Von Solms & Van Niekerk, 2013).

A practical example of this approach is the Digital Operational Resilience Act (DORA), which the European Commission considers as a tool to ensure the digital operational resilience of the financial sector. Within the framework of this regulation, digital resilience is defined as the ability of financial institutions to withstand serious ICT disruptions, including cyberattacks, and to continue providing key services without systemic disruption (DORA, 2025, January 17). A similar logic is embedded in the Cyber Resilience Act, which establishes mandatory cybersecurity requirements for digital products throughout their life cycle and places responsibility for a basic level of security on the manufacturers of digital solutions (European Commission, 2022, September 15). Thus, in the conceptual vision of the European Commission, cybersecurity is a necessary, but not exhaustive, component of digital resilience. While cybersecurity focuses on protectting against threats and minimizing vulnerabilities, digital resilience encompasses a broader range of tasks, including incident management, disaster recovery, institutional coordination, and long-term adaptation of digital systems (Christen et al., 2020). This integrated approach allows the European Union to view digital security not as a static state, but as a dynamic process, which is a key factor for the EU's competitiveness, strategic autonomy, and resilience in the face of growing hybrid threats (European Commission, n. d.).

2. Assessing cybersecurity in the EU digital environment

In the conceptual dimension, it is appropriate to distinguish between cybersecurity as a system of instruments and cyber incidents as a factor of dynamic change. Cybersecurity functions as an institutionally and technologically structured toolkit encompassing regulatory and legal mechanisms, organizational procedures, response algorithms, technical protection measures, and system recovery protocols.

At the same time, cyber incidents (cyberattacks, unauthorized intrusions, data breaches) act as a driving force that exposes vulnerabilities and stimulates the modernization of this toolkit. It is precisely real-world

incidents that generate the empirical basis for revising security standards, refining risk management models, and strengthening the institutional capacity of both the state and the private sector.

Thus, cybersecurity is not a primary causal factor but rather an adaptive system of measures that evolves in response to the growing complexity and intensity of cyber incidents.

The modern digital environment is characterized by high dynamics of development and a simultaneous increase in the scale and complexity of cyber incidents. Cyber incidents cover a wide range of threats, from unauthorized access and malware to targeted attacks on critical infrastructure and data manipulation. Their nature is increasingly determined by the use of artificial intelligence, automation of attacks, the use of social engineering and the exploitation of vulnerabilities in global digital supply chains.

The analysis of cybersecurity in the EU digital environment demonstrates its key role in ensuring the stable functioning of economy, public administration and society in the context of rapid digitalization. The EU considers cybersecurity as a component of strategic autonomy and digital resilience, which is reflected in the formation of a comprehensive regulatory framework, in particular the NIS2 Directive, the Cyber Resilience Act and the General Data Protection Regulation (GDPR).

The main challenges for cybersecurity in the EU remain the increasing number and sophistication of cyberattacks, in particular against critical infrastructure, the financial sector, government information systems and supply chains, as well as hybrid threats in the context of geopolitical instability (Cyble, 2024, December 5). In response, the EU is strengthening coordination between Member States, increasing institutional capacity of the European Cybersecurity Agency (ENISA), investing in cyber education, innovation and joint incident response mechanisms. At the same time, the analysis shows that the level of cybersecurity in EU countries is uneven, which necessitates the need to harmonise standards, exchange best practices and support less resilient digital systems. Thus, cybersecurity in the EU's digital environment appears not only as a technical task, but as a multidimensional policy aimed at ensuring trust in digital technologies, protecting citizens' rights, and increasing the overall resilience of the EU.

It is advisable to analyse cybersecurity in the EU digital environment using the Cybersecurity Index and the Cyber-dependent Crimes Index (ENACT Programme (n.d.), that allow assessing the state of cybersecurity and the real level of cyber threats in countries (*Table 2*). The Cybersecurity Index (FM Global, n. d.) is developed by the international insurance and analytical company FM Global and is aimed at assessing the readiness of countries to counteract cyber risks at the systemic level. The index reflects the structural ability of the state to prevent cyberattacks and minimize their consequences through the development of the institutional framework, regulatory framework, digital infrastructure, and the level of cyber protection of business and the public sector. In the EU context, this index often

correlates with the level of digital maturity, the quality of public administration, and investments in cyber resilience.

The Cyber-dependent crimes Index (ENACT Programme, n. d.), in turn, focuses not on readiness, but on the actual rate of cyber-dependent crime, i.e. crimes that cannot be committed without the use of digital technologies (hacking attacks, system hacking, malware, digital fraud, etc.). The Cyber-dependent crimes Index reflects the practical intensity of cyber threats and is an indicator of the real pressure of cybercrime on the economy, state institutions and society. For countries with a high level of digitalization, this index is often higher, which indicates an increase in the "attack surface" and the attractiveness of such states for cybercriminals.

Table 2

EU member states in Cybersecurity Index and Cyber-dependent crimes Index, 2025

Rank	Country	Cybersecurity Index (1–100 points)	Country	Cyber-dependent crimes Index (1–10 points)
1	Greece	99.6	Estonia	7
2	Cyprus	97.4	Netherlands	7
3	Luxembourg	95.5	Germany	7
4	Estonia	93.7	Belgium	6.5
5	Germany	93.4	France	6.5
6	Denmark	92.5	Denmark	6.5
7	Slovenia	92.1	Sweden	6.5
8	Finland	91.9	Spain	6.5
9	Netherlands	91.7	Romania	6
10	Italy	91.6	Italy	6
11	Malta	91.6	Ireland	6
12	Slovakia	91.2	Slovakia	6
13	Poland	91.0	Poland	6
14	Belgium	90.9	Bulgaria	6
15	Spain	89.8	Latvia	6
16	Lithuania	89.3	Lithuania	5.5
17	Romania	89.1	Hungary	5.5
18	France	88.9	Malta	5.5
19	Sweden	88.0	Finland	5.5
20	Ireland	87.2	Austria	5.5
21	Czech Republic	85.4	Czech Republic	5.5
22	Croatia	85.2	Portugal	5.5
23	Hungary	82.9	Croatia	5
24	Latvia	78.1	Slovenia	5
25	Austria	76.9	Greece	4.5
26	Bulgaria	72.1	Cyprus	4.5
27	Portugal	65.0	Luxembourg	4.5
EU average		88.2	EU average	5.8

Source: FM Global (n. d.); ENACT Programme (n. d.).

The average Cybersecurity Index score across the EU (see *Table 2*), indicating an overall high level of institutional and technical preparedness of the Member States to counter cyber risks. The leaders in this indicator are Greece, Cyprus and Luxembourg, which demonstrate almost maximum index values, which is the result of targeted public investments in national cybersecurity strategies, regulatory support and coordination with European institutions. At the same time, 9 EU countries have lower than the average level of cybersecurity for the EU, which indicates certain imbalances within the integration group. Analysis of the Cyber-dependent crimes Index shows that the there is a noticeable differentiation between countries. The highest values were recorded in Estonia, the Netherlands and Germany, which, despite the high positions of these countries in the cybersecurity ranking, indicates increased vulnerability to cybercrime, due to the high level of digitalization of the economy, the development of electronic services and a significant concentration of digital assets (European Commission, 2026). In contrast, countries with lower cybercrime rates, in particular Greece, Cyprus and Luxembourg, have a high level of cybersecurity.

Comparing both indices allows us to conclude that there is no direct linear relationship between the level of cybersecurity and the scale of cyber-related crimes in EU countries. On the contrary, in highly developed digital economies, strengthening cybersecurity is often accompanied by an increase in the number or complexity of cyberattacks, which requires not only technical protection, but also the development of analytical, legal and international countermeasures. According to forecasts by the European Cybersecurity Agency (ENISA), by 2030, cyber threats in the EU will become systemic and will be determined by a combination of technical, organizational and social threats (*Figure*).

Cyberthreats to lookout for in the EU through 2030

Source: Cyble (2024, December 5).

The data presented shows that by 2030, cyber threats in the EU will be cross-sectoral in nature, going beyond purely technical problems. Attacks on supply chains and critical infrastructure are of particular danger, which can cause cascading disruptions in the economy and society. At the same time, the role of the human factor, staff shortages and the use of artificial intelligence as a tool of cybercrime is growing. Accordingly, this requires EU Member States to systematically invest in human capital, the regulatory framework, cyber security standards and coordination tools to ensure the resilience of digital infrastructure in the face of growing challenges.

3. The assessment of EU countries digital resilience

In EU countries, digital resilience is considered not only as a technical characteristic of IT infrastructure, but as a multidimensional phenomenon that combines cybersecurity, institutional capacity, regulatory framework, the level of digital skills of the population and the integration of digital technologies into the economy and public administration. EU leaders in the field of digital resilience, in particular the countries of Northern and Western Europe, are characterized by a high level of digitalization, developed mechanisms for managing cyber risks, effective interdepartmental coordination and active participation in joint EU initiatives. At the same time, significant asymmetry remains between Member States, due to different levels of investment in digital infrastructure, uneven training of personnel and unequal readiness to implement European regulatory acts, in particular NIS2 and the Cyber Resilience Act.

Against this background, the growth of cyber threats, the spread of cyber-related crimes, dependence on global IT suppliers and the vulnerability of critical infrastructure reinforce the need to ensure digital resilience as a component of the EU's strategic autonomy. In this context, DORA is a key element in shaping the digital resilience of the European Union, as it creates a single legal framework at the supranational level to ensure the operational digital resilience of the financial sector. An analysis of the role of DORA shows that the regulation of cyber resilience has shifted from fragmented national approaches to a systemic model of digital risk management, which covers IT risks, cyber incidents, business process resilience, supply chain security and interaction with external IT providers. DORA establishes common standards for ICT risk management, mandatory digital resilience testing mechanisms, a centralized incident reporting system, and enhanced oversight of critical digital service providers, which significantly reduces the level of regulatory fragmentation within the EU. In a strategic dimension, the regulation shifts the emphasis from reactive cybersecurity to proactive digital resilience, focused on the ability of financial systems not only to counter cyberattacks but also to maintain functionality in crisis conditions. Thus, DORA is not just a regulatory act of financial regulation, but an institutional

framework for the formation of EU digital resilience, integrating cybersecurity, risk management, and the stability of digital infrastructure into a single systemic model of long-term digital security.

The results of the assessment of the level of digital resilience (The European Digital Resilience Index) and readiness for open technologies (The European Open Technology Readiness Index) of EU countries in 2025 are presented in the *Table 3*, divided into three analytical groups (tiers): Leadership Tier, Specialized Contender and Untapped Potential. In combination, these indices allow identifying structural imbalances between EU countries, showing different models of digital resilience formation, and assessing the role of open technologies as a strategic factor in strengthening the digital security and sovereignty of the EU.

Table 3

European Digital resilience Index
and European Open Technology Readiness Index in 2025

Rank	Country	EDRIX (1–10 points)	EOTRIX (1–10 points)	Tier
1	Germany	7.80	7.71	Leadership Tier
2	Czech Republic	6.89	4.75	
3	Sweden	6.80	7.48	
4	Finland	6.66	7.94	
5	Estonia	6.65	6.47	
6	France	6.64	6.29	
7	Slovenia	6.50	5.43	
8	Netherlands	6.24	7.93	Specialized Contender
9	Poland	5.98	4.28	
10	Austria	5.97	4.38	
11	Luxembourg	5.65	4.93	
12	Latvia	5.40	5.06	
13	Hungary	5.27	3.23	
14	Slovakia	5.25	3.55	
15	Portugal	5.15	4.91	
16	Denmark	5.08	5.85	
17	Spain	4.78	4.86	
18	Bulgaria	4.67	3.72	Untapped Potential
19	Italy	4.64	4.12	
20	Romania	4.02	2.50	
21	Belgium	3.87	4.11	
22	Greece	3.77	3.25	
23	Lithuania	3.49	3.98	
24	Croatia	3.48	3.56	
25	Ireland	3.10	4.49	
26	Cyprus	3.04	2.59	
27	Malta	2.76	4.83	

Source: EDRIX (2025).

The European Digital Resilience Index (EDRIX) and The European Open Technology Readiness Index (EOTRIX) are developed and calculated by the independent European analytical initiative EDRIX Consortium, which

brings together experts in the field of digital policy, open technologies, economics and cyber resilience. The initiative is research and analytical in nature and is not an EU institution, but its methodology is focused on the EU's strategic goals, in particular digital sovereignty, strategic autonomy and digital resilience. The indices are calculated on the basis of open international and European statistical sources, expert assessments and comparative policy analysis, which ensures cross-country comparability of results.

EDRIX is a composite index designed to measure the overall level of digital resilience of EU countries. Its key feature lies in its focus not merely on the level of digitalization or cyber protection, but on a country's ability to independently design, implement, and sustain digital technologies over the long term, even under conditions of crisis, external pressure, or technological disruption. To this end, the index covers several interrelated dimensions, including digital public policy, the capacity of the public and private sectors, the development of the domestic technological and developer ecosystem, and the level of societal adoption to digital solutions. Thus, EDRIX makes it possible to assess not declarative intentions, but a country's actual structural readiness to ensure digital resilience.

EOTRIX, in turn, is a specialized derivative index that focuses on the readiness of countries to use open technologies as a basis for digital resilience. It is calculated with an emphasis on those components of the digital ecosystem that are directly related to open software, open standards and open innovation models. EOTRIX measures the readiness of public policy, environment and society as a whole to implement open-source solutions and reduce dependence on closed technological ecosystems. In a scientific context, this index is an indicator of the potential for digital autonomy, since open technologies are considered as a tool for increasing transparency, security and flexibility of digital systems.

The Leadership Tier group includes countries with high EDRIX values (above ~6.5), which indicates a well-established institutional, technological and regulatory framework for digital resilience. Germany, Sweden and Finland demonstrate balanced values of both indices, representing the use of a combination of developed digital infrastructure and active implementation of open technologies.

At the same time, the Czech Republic and Slovenia demonstrate an asymmetric development model, in which a sufficient level of digital resilience is not accompanied by a corresponding readiness for open technologies. Accordingly, this indicates the dominance of state-centric or more closed digital ecosystems, where the emphasis is on protection and control, rather than on openness and innovative interaction.

The Specialized Contender group is characterized by medium EDRIX values (mainly 5.0–6.2) and significant EOTRIX variability. An example of this is the Netherlands, where with a medium level of digital resilience the country has one of the highest indicators of readiness for open technologies.

This result indicates an innovation-oriented model, where openness and technological integration are ahead of digital resilience. In contrast, Poland, Austria, Hungary and Slovakia demonstrate moderate EOTRIX values with medium level of EDRIX, which indicates a fragmented digital transformation and limited use of open technology solutions. Such a development structure may reduce the adaptability of digital systems in the long term.

The countries in the Untapped Potential group are characterized by moderate values of both indices, which indicates an insufficiently developed digital infrastructure, weak institutional mechanisms and limited integration into open technology ecosystems. Romania, Greece, Cyprus and Bulgaria demonstrate the lowest EOTRIX values, which indicates structural barriers to the implementation of open standards and digital innovations.

At the same time, some countries in this group, in particular Ireland and Malta, have relatively higher EOTRIX values with moderate EDRIX, which indicates the presence of technological potential without an appropriate level of digital resilience. Such a disparity increases the vulnerability of digital systems to crisis phenomena.

In general, the analysis shows that high readiness for open technologies does not always correlate with high digital resilience. In a number of countries, a clear asymmetry between these indicators is observed. Thus, digital resilience without technological openness can lead to innovation inertia, while openness without resilience can lead to increased systemic risks.

Conclusions

In theoretical understanding, cybersecurity and digital resilience are in a relationship of complementarity. Cybersecurity is a necessary functional component of digital resilience, providing protection against cyberattacks and unauthorized interference, while digital resilience covers a wider range of tasks, including crisis management, incident recovery and strategic adaptation to new threats. Both concepts are related to ensuring the reliable functioning of information and communication systems, data and digital services.

At the same time, cyber incidents exert a decisive influence on the development of digital resilience, as they expose existing vulnerabilities and generate momentum for revising risk management approaches. In effect, the evolution of cybersecurity occurs under the pressure of real-world threats.

Each large-scale cyber incident becomes a catalyst for updating standards, tightening regulatory requirements, modernizing technical solutions, and improving institutional response mechanisms. Thus, within the digital environment, a distinct principle of adaptive evolution operates: threats stimulate the advancement of protective instruments, while a system's capacity to withstand cyber incidents ultimately determines the level of its digital resilience.

To analyse cybersecurity in the EU digital environment, the Cybersecurity Index and the Cyber-dependent Crimes Index were considered as complementary analytical tools. High values of the cybersecurity index are not always accompanied by low levels of cybercrime, especially in countries with a

developed digital economy, which indicates the absence of a direct linear relationship between these indicators. Instead, such a comparison made it possible to identify structural features. Countries where a strong cybersecurity system is combined with a high level of cybercrime require attention to the implementation of preventive and analytical mechanisms, while countries with low indicators of both indices have a risk of hidden vulnerability due to insufficient digital integration and institutional framework.

The conducted analysis of The European Digital Resilience Index (EDRIX) and The European Open Technology Readiness Index (EOTRIX) indicates the presence of significant differences in the level of digital resilience and technological readiness of EU countries. In general, there is a clear differentiation of states by development levels, which allows for the identification of groups of leaders, specialized contenders, and countries with unrealized potential. Accordingly, 7 countries are included in the Leadership Tier group, 10 countries – Specialized Contender, 10 countries – Untapped Potential.

The examples of Greece, Malta and Cyprus demonstrate that a high level of cybersecurity does not always transform into a high level of digital resilience, which is due to the influence of institutional, technological and systemic factors. At the same time, the examples of Germany, Finland, Estonia, and Slovenia, which are characterized by high EDRIX and Cybersecurity Index results, indicate that digital resilience is formed under the influence of real cyber incidents in combination with institutional capacity, technological readiness, and the ability to restore digital systems, which allows us to confirm the hypothesis of the article.

Future research will involve the detailed modelling of sector-specific digital resilience parameters for critical infrastructure aimed at analysing industry-specific operational resilience indicators.

REFERENCES

Bada, M., & Agrafiotis, I. (2021). Cybersecurity capacity building: Assessing the knowledge and awareness of users. *Journal of Cyber Policy, 6*(3), 312–330. https://doi.org/10.1080/23738871.2021.2005018

Biliavskyi, V., Biliavska, Ya., Umantsiv, Yu., Shestack, Ya., Zhurba, O., & Khavanov, A. (2024). Digital Technologies in the Financial Sector of the Economy. *Financial and credit activity problems of theory and practice, 4*(57), 171–183. https://doi.org/10.55643/fcaptp.4.57.2024.4444

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of common market studies*. https://doi.org/10.1111/jcms.13654

Christen, M., Gordijn, B., & Loi, M. (Eds.). (2020). The ethics of cybersecurity. The International Library of Ethics, *Law and Technology*. https://duikt.edu.ua/uploads/l_2205_19674642.pdf

Cyble. (2024, December 5). EU cybersecurity in 2024: Insights from ENISA's latest report. https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report/

Digitaleurope. (2023, March 6). The digital front line: 15 actions to boost Europe's digital resilience. https://www.digitaleurope.org/news/the-digital-front-line-15-actions-to-boost-europes-digital-resilience/

DORA. (Digital Operational Resilience Act). (2025, January 17). *European Commission*. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

EDRIX. (2025). The European Digital Resilience Index 2025: A new barometer for sovereignty. https://edrix.eu/en/report

ENACT Programme. (n. d.). Global Organized Crime Index. https://ocindex.net/

ENISA Threat Landscape. (2025). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

European Commission. (2020). EU Cybersecurity strategy for the digital decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Commission. (2022, December 14). Directive (EU) 2022/2555 (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

European Commission. (2022, September 15). Cyber Resilience act – impact assessment. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment?utm_source=chatgpt.com

European Commission. (2025, December). Cyber resilience act. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Commission. (2026). Estonia 2025 Digital decade country report. https://digital-strategy.ec.europa.eu/en/factpages/estonia-2025-digital-decade-country-report

European Commission. (n. d.). EU cybersecurity policies. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

FM Global. (n. d.). FM Resilience Index: explore the data. https://www.fm.com/resources/resilience-index/explore-the-data/

Kerttunen, M. (2024). The EU Cyber Resilience Act: Horizontal cybersecurity requirements for products with digital elements. *European law journal*, *30*(1), 45–62.

Rotar, N. (2025). Cybersecurity and resilience in the structure of digital policy of the Visegrad Group countries. *Mediaforum: analytics, forecasts, information management*, (17), 205–226. https://doi.org/10.31861/mediaforum.2025.17.205-226

Sorokina, A., Lebedeva, L., & Lositska, T. (2024). Digital determinants of national economy resilience. *Baltic journal of economic studies*, *10*(5), 353–363. https://doi.org/10.30525/2256-0742/2024-10-5-353-363

T. Alcalá, Andra. (2025, June 5). *Strengthening the EU Cybersecurity Act: Strategic Recommendations for Coherence, Certification, and Systemic Resilience*. Available at SSRN: https://ssrn.com/abstract=5326851 or http://dx.doi.org/10.2139/ssrn.5326851

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, (38), 97–102. https://doi.org/10.1016/j.cose.2013.04.004

WEF (World Economic Forum). (2025). Global cybersecurity outlook 2025: Navigating the systemic risks of the AI era. https://www.weforum.org/reports/global-cybersecurity-outlook-2025/

Conflict of interest. The authors certify that they have no financial or non-financial interest in the subject matter or materials discussed in this manuscript; the authors have no association with state bodies, any organizations or commercial entities having a financial interest in or financial conflict with the subject matter or research presented in the manuscript. Given that the authors are affiliated with the institution that publishes this journal, which may cause potential conflict or suspicion of bias and therefore the final decision to publish this article (including the reviewers and editors) is made by the members of the Editorial Board who are not the employees of this institution.

The contribution of the authors is equal

Shkuropadska, D., & Lebedeva, L. (2026). Digital resilience and cybersecurity of EU countries. *Scientia fructuosa, 3*(167), 142–157. http://doi.org/10.31617/1.2026(167)08

Received by the editorial office 09.02.2026.
Sent for revision 13.03.2026.
Accepted for printing 24.04.2026.
Published online 19.06.2026.