NATIONAL UNIVERSITY
"YURI KONDRATYUK POLTAVA POLYTECHNIC"

Environmental, economic and information security of Ukraine in cooperation with EU:
challenges and perspectives

MONOGRAPH



ENVIRONMENTAL SECURITY | ECONOMIC SECURITY | INFORMATION SECURITY

Onyshchenko Svitlana, Maslii Oleksandra, Hlushko Alina, Maksiuta Nataliia

ENVIRONMENTAL, ECONOMIC AND INFORMATION SECURITY OF UKRAINE IN COOPERATION WITH EU: CHALLENGES AND PERSPECTIVES

Included in International scientometric databases

MONOGRAPH

Co-funded by the European Union

ScientificWorld-NetAkhatAV
Karlsruhe 2026

UDC 338.246.8:502.1:004.056](477):339.924(4-6ЄС)

Recommended for publication by the decision of the Academic Council of the National University "Yuri Kondratyuk Poltava Polytechnic" (Minutes No. 12 dated September 18, 2026)

Reviewer:

Mioara-Florina Pantea – PhD in Economics, Associate Professor, Dean of the Faculty of Economic Sciences, "Aurel Vlaicu" University of Arad, Arad, Romania;

Inna Stecenko – Doctor of Economics, Professor, Head of the PhD Programme "Digital Economy and Business", Chairwoman of the Promotion (Doctoral) Council "Economics and Business", Transport and Telecommunication Institute (Riga, Latvia), Expert of the United Nations Environment Programme (UNEP), Expert of the World Bank (B-READY 2026);

Hanna Yarovenko – D.Sc., Visiting Professor, Department of Computer Science and Engineering, Carlos III University of Madrid, Spain.

Authors:

Svitlana Onyshchenko – Doctor of Economics, Professor, Director of the Educational and Scientific Institute of Finance, Economics, Management and Law, National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine. ORCID 0000-0002-6173-4361

Oleksandra Maslii – PhD in Economics, Associate Professor, Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine. ORCID 0000-0003-2184-968X

Alina Hlushko – PhD in Economics, Associate Professor, Leading Research Fellow of the Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine. ORCID 0000-0002-4086-1513

Nataliia Maksiuta – PhD, Senior Lecturer of the Department of Applied Ecology and Chemistry, National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine. ORCID 0000-0002-0256-6986

Environmental, Economic and Information Security of Ukraine in Cooperation with EU: Challenges and Perspectives [Text] : Monograph / S. Onyshchenko, O. Maslii, A. Hlushko, N. Maksiuta. Karlsruhe, 2026. 145 p. (Electronic edition)

The monograph "Environmental, Economic and Information Security of Ukraine in Cooperation with EU: Challenges and Perspectives" was prepared within the framework of the Jean Monnet Module "Ensuring environmental, economic and information security: EU experience for Ukraine" (101127395 – EEEISEUEU – ERASMUS-JMO-2023-HEI-TCH-RSCH).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Education and Culture Executive Agency (EACEA). Neither the European Union nor the granting authority can be held responsible for them.

ISBN 978-3-98924-174-9
DOI: 10.30890/978-3-98924-174-9.2026

Published by:

ScientificWorld-NetAkhatAV
Lußstr. 13
76227 Karlsruhe, Germany

Copyright © Onyshchenko S., Maslii O., Hlushko A., Maksiuta N. 2026

CONTENTS

PREFACE 4

CHAPTER 1. THE EUROPEAN SECURITY SPACE AND STRATEGIC ORIENTATIONS FOR UKRAINE'S INTEGRATION 7
1.1. European Union security policy amidst global challenges 8
1.2. EU-Ukraine Partnership in the Field of Security 23
1.3. Roadmap for Ukraine's integration into the European security space 30

CHAPTER 2. ENVIRONMENTAL SECURITY IN UKRAINE IN THE CONTEXT OF THE EUROPEAN GREEN DEAL 43
2.1. The European Green Deal as a strategic framework for environmental transformation 44
2.2. Harmonisation of Ukraine's environmental policy and EU legislation 49
2.3. Environmental threats and challenges in Ukraine in the context of the war 53
2.4. Ukraine's green post-war recovery: implementing European climate and ecological standards 58

CHAPTER 3. UKRAINE'S ECONOMIC SECURITY WITHIN THE FRAMEWORK OF EUROPEAN ECONOMIC STABILITY 65
3.1. Strategic Guidelines for the Economic Security of the European Union 66
3.2. Threats to Ukraine's economic security in the context of war and European integration 78
3.3. Forming an ecosystem of economic resilience to hybrid threats: European experience and opportunities for its implementation in Ukraine 88

CHAPTER 4. INFORMATION AND CYBERSECURITY OF UKRAINE IN THE ARCHITECTURE OF EUROPEAN DIGITAL RESILIENCE 99
4.1. Institutional framework for ensuring information security and digital resilience of the European Union 100
4.2. Transformation of information threats to Ukraine and the EU in the context of hybrid and full-scale war 110
4.3. Strategic partnership between Ukraine and the European Union in the field of cybersecurity: institutional mechanisms and development directions 119
4.4. Digital integration of Ukraine into the European Union: security imperatives, risks and strategic prospects 126

APPENDICES 139

PREFACE

Ukraine's European integration is taking place under conditions unprecedented in the history of European Union enlargement. A state resisting full-scale armed aggression is simultaneously conducting accession negotiations, implementing far-reaching reforms and approximating its national legislation to EU law. At the same time, the European Union itself is rethinking its security policy: it is moving from crisis management towards strategic resilience and comprehensive preparedness, while economic, climate, cyber and digital security issues are increasingly governed by common legal instruments. Under these circumstances, Ukraine's integration into the European security space is no longer a distant prospect but is acquiring a practical dimension. This calls for scholarly reflection both on the logic of the transformation of EU security policy and on the mechanisms through which Ukraine can gradually become a full participant in it.

This monograph examines the European security space and the strategic guidelines for Ukraine's integration into it. The first chapter analyses the evolution of EU security policy in the context of global challenges; explores the substance of the Strategic Compass, the EU Economic Security Strategy and the legal architecture of economic, climate, cyber and digital security; systematises the stages and instruments of the EU-Ukraine security partnership; and proposes a roadmap for Ukraine's integration into the European security space based on adaptive implementation. The subsequent chapters address the digital dimension of Ukraine's European integration. The monograph is intended for researchers, experts and practitioners in public administration and international relations, as well as for university teachers, doctoral students and students engaged in the study of economic security and European integration.

The second chapter provides a comprehensive analysis of the theoretical and practical foundations for ensuring Ukraine's environmental security in the context of European integration, the implementation of the European Green Deal and the country's post-war recovery. It highlights the role of the green transformation of the economy, the harmonisation of environmental policy and legislation with European Union law, the development of environmental monitoring systems, and the introduction of innovative technologies and mechanisms for managing environmental

resources to achieve sustainable development goals. The study analyses the environmental threats caused by full-scale war, their impact on natural ecosystems, economic, food and national security, as well as approaches to assessing and documenting environmental damage. The importance of implementing the principles of green recovery, low-carbon development and adaptation to climate change, based on European environmental standards, is demonstrated as key prerequisites for strengthening environmental and energy security, enhancing economic resilience and ensuring Ukraine's long-term sustainable development.

Chapter three examines the economic security of Ukraine within the framework of European economic stability. It analyses the strategic guidelines underpinning the European Union's economic security policy, including the triad of promoting competitiveness, protecting against risks and building partnerships, together with the corresponding institutional and regulatory architecture developed at the supranational level. It identifies and systematises the principal threats to Ukraine's economic security arising from the war and from the deepening of European integration processes, including disruptions to production and trade, energy and resource dependencies, and the erosion of critical infrastructure and human capital. It substantiates an ecosystem-based approach to building economic resilience to hybrid threats, drawing on European experience in risk assessment, critical-infrastructure protection and information-space resilience, and outlines the preconditions and mechanisms for adapting this experience to Ukrainian practice.

Chapter four presents a comprehensive analysis of the institutional, legal, and organizational frameworks for ensuring Ukraine's information and cybersecurity within the context of European integration and the development of digital resilience. It examines the specific features of the institutional-legal and institutional-organizational arrangements for information security within the European Union. The chapter analyzes the evolving nature of information threats facing Ukraine and the EU amidst hybrid and full-scale warfare – specifically the evolution of disinformation campaigns, FIMI operations, networked forms of information influence, and the use of cutting-edge digital technologies to manipulate public opinion and undermine trust in democratic institutions. It explores the development of the strategic partnership between Ukraine and the EU in the cybersecurity sphere, encompassing political dialogue, regulatory alignment, institutional interaction, operational-technical cooperation, cyber-capacity building, and cyber-solidarity mechanisms. The study argues that deepening Ukraine's digital integration with the EU requires not only adaptation to the digital acquis but also the assurance of regulatory, institutional, technological, and infrastructural interoperability. Finally, it identifies key security imperatives, risks, and strategic prospects associated with Ukraine's digital integration into the European Union. It has been established that

strengthening information and cybersecurity must be viewed as an essential prerequisite for Ukraine's further integration into the European digital space, and that the combination of regulatory alignment, institutional cooperation, technological interoperability, and joint response mechanisms forms the foundation for enhancing digital resilience, protecting national interests, and deepening Ukraine's European integration.

The monograph "Environmental, Economic and Information Security of Ukraine in Cooperation with EU: Challenges and Perspectives" was prepared within the framework of the Jean Monnet Module "Ensuring environmental, economic and information security: EU experience for Ukraine" (101127395 – EEEISEUEU – ERASMUS-JMO-2023-HEI-TCH-RSCH, 2023–2026), implemented by the Educational and Research Institute of Finance, Economics, Management and Law of National University "Yuri Kondratyuk Poltava Polytechnic".

Funded by the European Union. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

CHAPTER 1

THE EUROPEAN SECURITY SPACE AND STRATEGIC ORIENTATIONS FOR UKRAINE'S INTEGRATION



1.1. European Union security policy amidst global challenges

The research of the European Union's security policy requires a clear definition of its theoretical foundations, as it is precisely the understanding of the nature of security that determines the boundaries of the European security space and the scope of candidate states' integration into it. In the classical realist tradition, security was equated with the military defence of a state's territory and sovereignty. This perspective prevailed in European thinking throughout the "Cold War", when NATO fulfilled the function of collective defence, whilst European communities focused on economic integration. The end of the bipolar confrontation broke down this functional boundary and confronted Europe with the question of its own role in ensuring security.

The Copenhagen School of security studies established one of the conceptual foundations for an expanded interpretation of security. Barry Buzan, Ole Wæver, and Jaap de Wilde proposed analyzing security across five interconnected sectors: military, political, economic, societal, and environmental [1]. Of fundamental importance to our study is the theory of securitization developed within the Copenhagen School; according to this theory, an issue acquires "security" status not automatically due to its objective characteristics, but rather through its framing as an existential threat – a process that justifies measures extending beyond the scope of ordinary politics. Applying this perspective to the evolution of European Union policy makes it possible to trace the gradual incorporation of energy dependence, supply chain vulnerabilities, climate change, cyber threats, and foreign information manipulation and interference into the scope of European security policy.

A second theoretical approach is provided by Ulrich Beck's concept of the «risk society». According to this concept, modern modernization itself generates global-scale risks that transcend national borders and cannot be neutralized by the actions of any single state [2]. This provides a rationale for a supranational level of security governance, which the EU implements by combining the Common Foreign and Security Policy with regulatory powers in areas such as the internal market, energy, the environment, and the digital economy.

The normative foundation of EU security policy is established in the founding treaties. Article 21 of the Treaty on European Union identifies the preservation of peace, the prevention of conflicts, and the strengthening of international security among the objectives of the Union's external action [3, Art. 21(2)]. Article 42 enshrines

the Common Security and Defence Policy as an integral part of the Common Foreign and Security Policy and provides for the gradual framing of a common EU defence policy [3, Art. 42(2)]. The mutual assistance clause is of particular importance: in the event of armed aggression against a member state's territory, other member states are obliged to provide aid and assistance by all the means in their power, in accordance with Article 51 of the UN Charter [4, Art. 51]. Alongside the mutual assistance provision, the solidarity clause – enshrined in Article 222 of the Treaty on the Functioning of the European Union – plays a significant role; under this clause, the Union and its Member States act jointly in a spirit of solidarity in the event of a terrorist attack or a natural or man-made disaster [5, Art. 222]. Together, these provisions form a complementary legal framework for European security: a defense dimension addressing armed aggression against a Member State, and a crisis-solidarity dimension focused on responding to terrorist threats and natural or man-made disasters.

A turning point in the conceptualization of EU security was the 2016 Global Strategy for the European Union's Foreign and Security Policy, titled "Shared Vision, Common Action: A Stronger Europe". The document introduced the principle of "principled pragmatism" and outlined five priorities for external action: the security of the Union; the resilience of states and societies to the east and south; an integrated approach to conflicts and crises; cooperative regional orders; and global governance for the 21st century [6]. A key innovation was the concept of resilience, which the strategy defines as the ability of states and societies to reform while withstanding and recovering from internal and external crises.

Scholarly assessment of this conceptual shift is mixed. A. Juncos views it as a pragmatic turn in which the EU abandons the ambition of transforming partners in its own image in favor of supporting their capacity to withstand shocks [7]. While acknowledging the concept's heuristic potential, W. Wagner and R. Anholt warn that its excessive breadth risks turning resilience into a slogan devoid of operational substance [8].

Economic resilience theory offers a response to this concern. R. Martin and P. Sunley distinguish three types: engineering resilience, defined as the speed at which a system returns to its pre-crisis equilibrium; ecological resilience, the capacity to absorb shocks without shifting to a qualitatively different state; and adaptive – or transformational – resilience, understood as the long-term restructuring of a system in response to structural changes [9]. This typology makes it possible to operationalize a concept that is often used in EU policy documents without a clear definition, and to link it to measurable characteristics of economic systems. In our view, the subsequent evolution of EU policy has largely addressed concerns regarding the concept's vagueness, particularly because, after 2020, resilience was given concrete operational substance through specific regulations and directives.

The institutionalization of resilience as a cross-cutting principle took place in documents issued in 2020. The 2020 Strategic Foresight Report proposed analyzing EU resilience across four interconnected dimensions: social and economic, geopolitical, green, and digital [10]. The EU Security Union Strategy for 2020–2025 integrated internal and external security into a single framework for the first time and established priorities that included critical infrastructure protection, cybersecurity, and countering hybrid threats [11]. It is important to note that European security policy in the 21st century is being shaped by new challenges and threats that require a comprehensive approach to ensuring the continent's stability. The European Union's Common Security and Defence Policy (CSDP), as an integral part of the Common Foreign and Security Policy (CFSP), serves as the primary framework for coordinating member states' security efforts.

Russia's full-scale aggression against Ukraine in 2022 triggered a significant acceleration in EU security policy. The Versailles Declaration issued by heads of state or government on March 10-11, 2022, identified three interconnected dimensions for strengthening European sovereignty: bolstering defense capabilities, reducing energy dependencies, and building a more robust economic base [12]. Notably, these three dimensions directly correlate with defense, energy-environmental, and economic security, thereby demonstrating the EU's shift toward an integrated understanding of security at the highest level of political decision-making.

At the same time, empirical studies demonstrate that, even with shared institutional frameworks, the resilience of member states to external shocks remains asymmetric. Applying a vector error correction model to quarterly Eurostat data (2015–2024) for the Eurozone as a whole, as well as for Germany, France, Spain, and Greece, A. Anagnostou and N. Galatis found that core economies exhibit more restrained and coordinated adjustment, whereas peripheral economies are characterized by higher fiscal sensitivity, more protracted labor market adaptation, and stronger macroeconomic interdependence [13]. Notably, the COVID-19 pandemic shock triggered systemic effects across almost all the economies studied – primarily through production contractions and deteriorating public finances – while the geopolitical shock stemming from Russia's aggression against Ukraine propagated in a far more uneven manner; this highlights the role of national structural characteristics in shaping adaptive capacity [13]. The authors conclude that resilience within a monetary union should be understood not merely as a return to equilibrium, but as the stability, coordination, and durability of the entire adjustment process, although they emphasize the descriptive rather than causal nature of their findings. In our view, this conclusion holds broader significance for the theory of the European security space: common rules and instruments are a necessary but insufficient condition for resilience, as the latter is also determined by national institutional and structural capacities. For Ukraine as a future member state, this implies that integration into the European security space must

be accompanied by the strengthening of its own mechanisms for fiscal stability and labor market adaptability – areas facing the greatest strain under wartime conditions.

The further evolution of the comprehensive resilience concept is evident in S. Niinistö's report "Safer Together" (2024), which substantiated a preparedness model based on a whole-of-government and whole-of-society approach [38], and in the 2025 Union Preparedness Strategy, which translates these principles into concrete actions – such as the recommendation to ensure the population's capacity to function autonomously for at least 72 hours during a crisis [31]. Thus, in less than a decade, EU security policy has shifted from crisis management to strategic resilience and comprehensive preparedness (Table 1.1).

Table 1.1

Evolution of Key Strategic Documents Shaping the EU Security Policy (2016–2025)

Document	Year	Type / Institutional Status of the Document	Conceptual Focus	Key Provisions
1	2	3	4	5
EU Global Strategy [6]	2016	Strategic document presented by the High Representative of the Union; its presentation was welcomed by the European Council	Resilience; principled pragmatism; integrated approach	Five priorities: the security of the Union; state and societal resilience; an integrated approach to conflicts and crises; cooperative regional orders; global governance based on rules
Strategic Foresight Report [10]	2020	Communication from the European Commission, COM(2020) 493 final	Resilience as a new compass for EU policymaking	Four interconnected dimensions of resilience: social and economic, geopolitical, green, and digital; integration of strategic foresight into EU policymaking
EU Security Union Strategy [11]	2020	Communication from the European Commission, COM(2020) 605 final	Comprehensive approach to security; interconnection between internal and external dimensions of security	Four priorities: a future-proof security environment; tackling evolving threats; protecting Europeans from terrorism and organised crime; building a strong European security ecosystem
Versailles Declaration [12]	2022	Declaration by EU leaders adopted at the informal meeting in Versailles	Strengthening European sovereignty and reducing strategic dependencies	Three key areas: strengthening defence capabilities; reducing energy dependencies; building a more resilient economic base
Strategic Compass [16]	2022	Action plan in the field of security and defence, approved by the Council of the EU	Strengthening the EU's capacity to act in security and defence; a «quantum leap»	Four strands: Act – Secure – Invest – Partner: act more rapidly and decisively; secure the EU; invest in capabilities and technologies; strengthen partnerships

1	2	3	4	5
European Economic Security Strategy [17]	2023	Joint Communication by the European Commission and the High Representative, JOIN(2023) 20 final	De-risking while preserving economic openness	Three priorities: Promote – Protect – Partner; four categories of risks: resilience of supply chains, physical and cyber security of critical infrastructure, technology security and technology leakage, and weaponisation of economic dependencies / economic coercion
White Paper for European Defence – Readiness 2030 [18]	2025	Joint White Paper, JOIN(2025) 120 final	European defence readiness by 2030	Seven priority capability areas: air and missile defence; artillery systems; ammunition and missiles; drones and counter-drone systems; military mobility; AI, quantum technologies, cyber and electronic warfare; strategic enablers and protection of critical infrastructure; deeper integration with Ukraine's defence industry
Preparedness Union Strategy [15]	2025	Joint Communication by the European Commission and the High Representative, JOIN(2025) 130 final	Comprehensive preparedness and resilience	Three core approaches: all-hazards, whole-of-government, whole-of-society; the principle of preparedness by design; seven areas of action: strategic foresight, resilience of vital societal functions, population preparedness, public-private cooperation, civil-military cooperation, crisis response, and resilience through external partnerships

Source: systematized by the authors from [6;10-12; 15-18]

The Strategic Compass for Security and Defence, approved by the Council of the EU on 21 March 2022 and endorsed by the European Council on 24–25 March 2022, occupies a distinctive place in the Union's security policy [16]. Unlike the Global Strategy, which was predominantly conceptual in nature, the Compass was conceived as an action plan setting out concrete measures and timelines up to 2030. Its stated objective is to make the EU a stronger and more capable security provider, able to protect its citizens and to contribute to international peace and security. Work on the document began well before the full-scale invasion and drew on the first-ever comprehensive EU threat analysis, conducted in November 2020 on the basis of intelligence assessments provided by the Member States. The final text, however, was adopted after the outbreak of the war, and this is reflected in its content: the document

characterises Russia's war of aggression as "a tectonic shift in European history" and argues that the more hostile security environment requires the EU to make a "quantum leap forward" by increasing its capacity and willingness to act, strengthening its resilience and investing more and better in defence capabilities.

The Compass is structured around four interrelated pillars: Act, Secure, Invest and Partner. In our view, this structure reflects a comprehensive understanding of security, ranging from the operational capacity to respond to crises to the long-term strengthening of the technological and industrial base and the development of partnerships (Fig. 1.1).

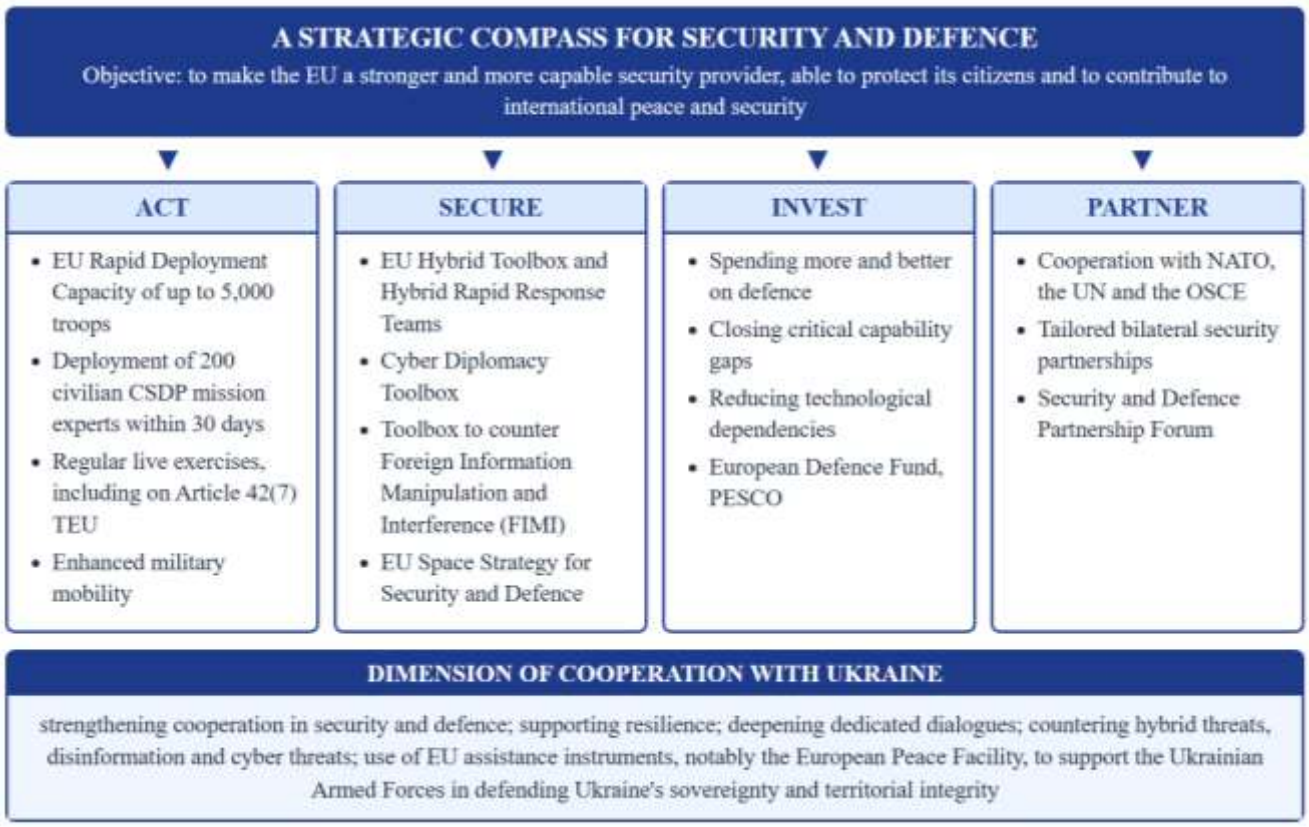


Fig. 1.1. Key instruments of the EU Strategic Compass by pillar
Source: compiled by the authors based on [16].

The "Act" strand aims to bridge the gap between the European Union's strategic ambitions and its actual operational capacity. The Strategic Compass itself acknowledges the EU's insufficient collective readiness to counter the full spectrum of modern threats and highlights the need to narrow the gap between stated aspirations and practical actions. Establishing an EU Rapid Deployment Capacity of up to 5,000 troops, ensuring the readiness to deploy up to 200 fully equipped CSDP civilian mission experts within 30 days, conducting regular exercises, and enhancing military

mobility are intended to strengthen the Union's ability to act swiftly and decisively – with partners whenever possible, and independently when necessary [16].

For Ukraine, the significance of this strand should be viewed in the context of progressively deepening operational cooperation with the EU. At the same time, the experience Ukraine has gained in high-intensity combat operations has taken on particular importance for the development of European defense capabilities in subsequent EU strategic documents. Notably, the 2025 White Paper on European Defence envisages utilizing relevant lessons to define the future defense needs of member states and develop their capabilities [16].

The «Secure» strand is of particular importance to this study, as it demonstrates how European security policy is moving beyond the traditional military-defense dimension. The Council of the EU conclusions of 21 June 2022 established a framework for a coordinated response to hybrid campaigns and detailed the «EU Hybrid Toolbox», which combines preventive, cooperative, and resilience-building measures with restrictive and other response instruments. In parallel, the development of the «FIMI Toolbox» created a dedicated toolkit for detecting, analyzing, and responding to foreign information manipulation and interference [19].

The cyber dimension was strengthened by the 2022 EU Cyber Defence Policy, while the protection of the space domain was addressed by the 2023 EU Space Strategy for Security and Defence. Collectively, these instruments demonstrate the gradual integration of the hybrid, cyber, and information dimensions into the Union's overall security system [20].

The "Invest" strand primarily encompasses the industrial, technological, and capability foundations of European security and defense. The Strategic Compass underscores the need to increase defence spending and enhance its efficiency, close critical gaps in military and civilian capabilities, develop next-generation defence technologies, and reduce strategic technological and industrial dependencies. The document also highlights the need to overcome fragmentation and develop a more coordinated European approach to building defense capabilities. This area saw its most dynamic development after 2022. The European defense White Paper «Readiness 2030», presented in March 2025, identified seven priority capability areas: air and missile defense; artillery systems; ammunition and missiles; unmanned and anti-drone systems; military mobility; artificial intelligence, quantum technologies, cyber capabilities, and electronic warfare; and strategic enablers and critical infrastructure protection [18].

SAFE (Security Action for Europe) – established by Regulation (EU) 2025/1106, became the financial instrument for strengthening this area; it provides up to €150 billion in loan financing to Member States for defense investments, primarily through joint procurement. At the same time, Ukraine can participate in such joint

procurements on equal terms with Member States and EEA/EFTA countries, and Ukrainian manufacturers can act as suppliers within the framework of these procurements [22].

Of particular importance for Ukraine's further integration is the fact that the White Paper explicitly orients EU policy toward deepening cooperation between the European and Ukrainian defense industries and integrating the Ukrainian defense industry into the European Defence Technological and Industrial Base (EDTIB). This approach is gradually transforming Ukraine's role from primarily a recipient of military support into a participant in the European system for developing defense capabilities and defense-industrial cooperation [23].

The «Partnership» track entails deepening multilateral cooperation and developing tailored bilateral partnerships with states that share EU interests and values. The Strategic Compass explicitly calls for strengthening cooperation with NATO, the UN, and other international and regional partners, as well as developing individualized cooperation formats with third countries. For Ukraine, a further practical manifestation of this logic was the Joint Security Commitments between the European Union and Ukraine, signed on June 27, 2024, which aim to strengthen Ukraine's long-term capacity for self-defense, countering destabilization, and deterring future aggression [16; 23].

When assessing the Strategic Compass as a whole, it is worth highlighting three characteristics that are essential for further analysis. First, the document establishes a regular mechanism for monitoring its implementation: the High Representative, in consultation with the European Commission and the European Defence Agency, is to present an annual progress report serving as a basis for political guidance from the European Council. Second, the Compass enshrines a comprehensive understanding of security, viewing military threats in conjunction with hybrid campaigns, cyberattacks, information manipulation, technological dependencies, climate risks, and other challenges. Third, the strengthening of the EU's strategic autonomy is not framed as an alternative to the transatlantic partnership. Instead, a stronger and more capable EU in the field of security and defence is regarded as complementary to NATO, which remains the cornerstone of collective defence for its members.

A distinctive feature of the EU as a security actor is that a significant portion of its security policy is implemented not through Common Foreign and Security Policy instruments, but through the regulation of the internal market, energy, the environment, and the digital economy. It is in these areas that the Union possesses the most comprehensive powers, and its legal acts have direct effect or are subject to mandatory transposition. Therefore, for a candidate state, integration into the European security space largely entails aligning with these acts.

The EU Economic Security Strategy, unveiled on June 20, 2023, was the first document to articulate the Union's holistic approach to this field [17]. Its methodological foundation is the concept of "de-risking", which stands in contrast to both a complete severing of economic ties and naive openness. The strategy rests on three pillars: promoting the EU's own competitiveness, protecting against risks, and cooperating with the broadest possible range of partners. It identifies four categories of risks: supply chain resilience (particularly regarding energy); the physical and cyber security of critical infrastructure; technological security and technology leakage; and the weaponization of economic dependencies and economic coercion. To assess technology risks, the Commission identified ten critical technology areas in its recommendation of 3 October 2023; four of these (advanced semiconductors, artificial intelligence, quantum technologies, and biotechnologies) were designated as priorities for immediate risk assessment [24].

The strategy is operationalized through a series of regulations. Regulation (EU) 2019/452, applicable since October 11, 2020, established a framework for screening foreign direct investments and identified factors that Member States and the Commission may consider – specifically, the impact of an investment on critical infrastructure, critical technologies, the supply of critical resources, access to sensitive information, and media freedom and pluralism [25, Art. 4]. Regulation (EU) 2023/2675 introduced the Anti-Coercion Instrument, providing the Union for the first time with a legal basis to respond to situations where a third country employs trade or investment measures to compel the EU or a Member State to adopt a specific decision [26]. The European Chips Act (Regulation (EU) 2023/1781) aims to strengthen the Union's semiconductor ecosystem and establish a mechanism for monitoring and responding to supply chain crises [27]. The Critical Raw Materials Act (Regulation (EU) 2024/1252) established benchmarks for 2030: EU extraction of at least 10%, processing of at least 40%, and recycling of at least 25% of the annual consumption of strategic raw materials, as well as a limit on dependency on any single third country to no more than 65% of the consumption of each strategic raw material at any stage of processing [28]. The latter provision is of direct relevance to Ukraine, which, back in 2021, signed a Memorandum of Strategic Partnership on raw materials, batteries, and renewable hydrogen with the EU [29] (Fig. 1.2).

The validity of the risk-reduction approach is also confirmed by data on the uneven distribution of geopolitical shocks within the EU. As demonstrated by A. Anagnostou and N. Galatis, the shock associated with Russia's aggression against Ukraine caused significantly more heterogeneous consequences across Eurozone states than the pandemic did [13]. Consequently, the Union's collective economic security requires not only supranational protection mechanisms but also the mitigation of structural vulnerabilities in individual member states.

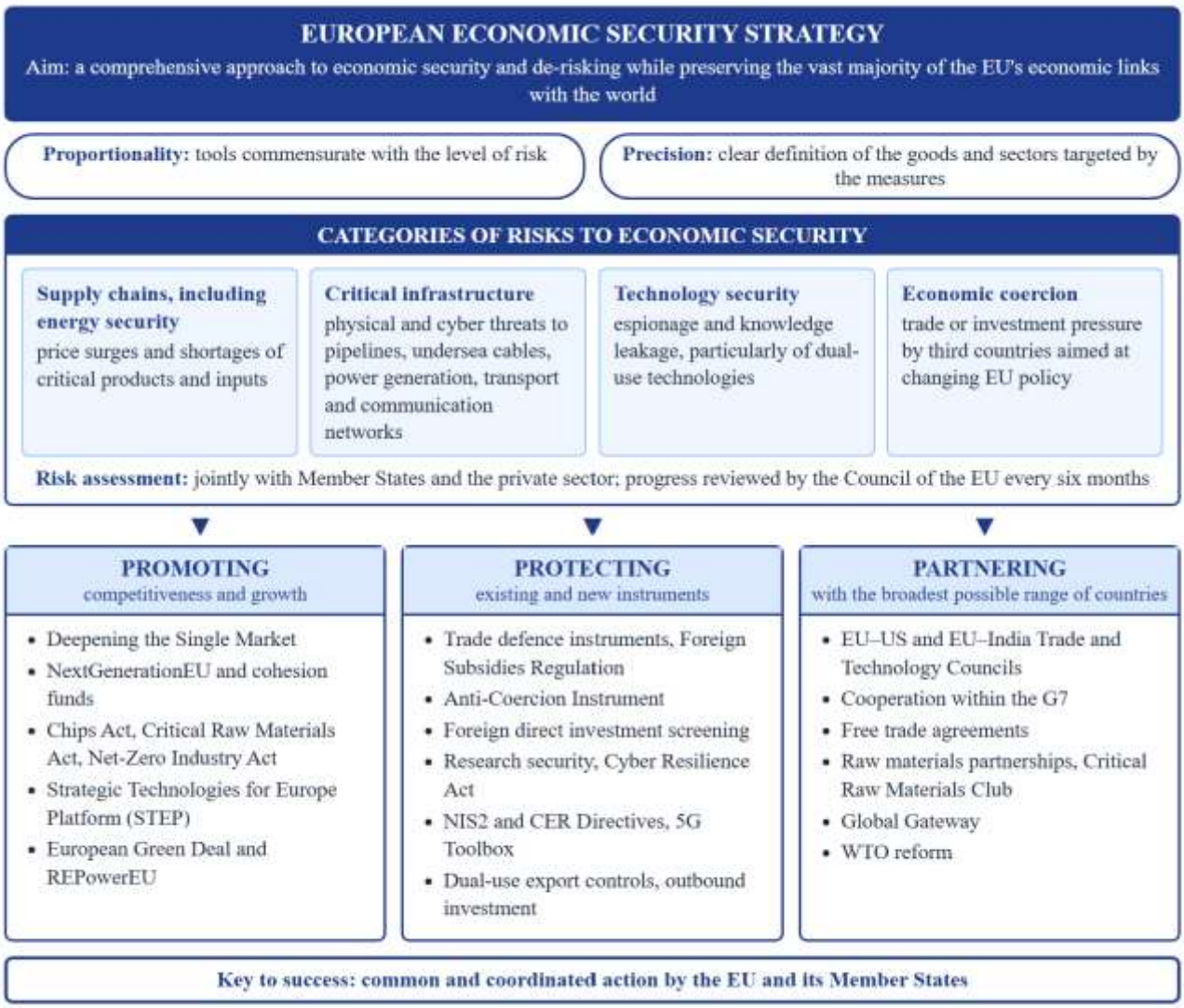


Fig. 1.2. Main strategic pillars and initiatives of the EU Economic Security Strategy
Source: compiled by the authors based on [17].

The 2019 European Green Deal [30] set the goal of transforming the EU into the world's first climate-neutral economy. This objective was enshrined in the European Climate Law, which commits the Union to achieving climate neutrality by 2050 at the latest [31, Art. 2] and reducing net greenhouse gas emissions by at least 55% by 2030 compared to 1990 levels [31, Art. 4(1)]. Regulation (EU) 2026/667, which entered into force on April 7, 2026, added a mandatory interim Union target to the Climate Law: a 90% reduction in net emissions by 2040 compared to 1990 levels [33]. Following 2022, environmental policy acquired a security dimension: the REPowerEU plan set the objective of rapidly phasing out Russian fossil fuels through energy conservation, supply diversification, and the accelerated development of renewable energy [32]. This logic is embedded in the revised Renewable Energy Directive, which established a mandatory target for the share of renewable sources in the EU's final energy consumption of at least 42.5% by 2030, with an ambition to reach 45% [34].

Environmental policy also gained an external economic dimension through the Carbon Border Adjustment Mechanism (CBAM). Regulation (EU) 2023/956 extends carbon pricing to imports of cement, iron and steel, aluminium, fertilizers, electricity, and hydrogen; The transition period ran from October 1, 2023, to December 31, 2025, with the definitive regime applying from 2026 [35]. For Ukraine, whose exports to the EU comprise a significant share of metallurgical products and fertilizers, CBAM turns climate standards into a factor of competitiveness and, consequently, economic security.

The EU's regulatory framework for digital and information security is the most extensive. Strategic direction is set by the Digital Compass 2030 [36], the goals of which became legally binding through the Decision establishing the Digital Decade Policy Programme 2030 [37, Art. 4]. The Decision sets targets in the areas of digital skills (at least 80% of individuals aged 16–74 with basic digital skills and 20 million employed ICT specialists), secure and sustainable digital infrastructure (gigabit connectivity for all end-users, 5G coverage for all populated areas, and an EU share of at least 20% in global advanced semiconductor production), business digital transformation (adoption of cloud computing, big data, or artificial intelligence by at least 75% of enterprises), and the digitalization of public services (100% online availability of key public services). Progress toward these goals is monitored via the annual «Report on the State of the Digital Decade» and the Member States' national strategic roadmaps.

The cybersecurity component relies on the NIS2 Directive, which was required to be transposed by October 17, 2024 [38]. The Directive extends cybersecurity requirements to essential and important entities across 18 sectors, mandating the implementation of cyber risk management measures [38, Art. 21] and establishes a phased procedure for reporting significant incidents: an early warning within 24 hours, incident notification within 72 hours, and a final report within one month [38, Art. 23]. In parallel, Directive (EU) 2022/2557 on the resilience of critical entities sets out physical resilience requirements for entities across 11 sectors, which Member States must identify by July 17, 2026 [39]. The new generation of cybersecurity acts comprises the Cyber Resilience Act, which introduces mandatory cybersecurity requirements for products with digital elements [40], and the Cyber Solidarity Act, which establishes the European Cyber Shield, the Cyber Emergency Mechanism, and the EU Cybersecurity Reserve [41].

The regulatory framework governing the digital environment of the European Union is formed, in particular, by the General Data Protection Regulation (GDPR) [42], the Digital Services Act (DSA) [43] and the Digital Markets Act (DMA) [44]. These acts cover interrelated yet distinct areas of regulation: the protection of personal data, the accountability of online intermediaries and the management of systemic risks, and ensuring fairness and contestability in digital markets. The Digital Services Act

requires very large online platforms and very large online search engines to assess systemic risks, including actual or foreseeable negative effects on democratic processes, civic discourse, electoral processes and public security [43, Art. 34], and establishes a crisis response mechanism [43, Art. 36]. The latter was incorporated into the DSA during the legislative negotiations in the context of Russia's aggression against Ukraine and the related manipulation of online information.

The Artificial Intelligence Act introduces a risk-based model for regulating AI. Its general date of application is 2 August 2026; the rules on general-purpose AI models have applied since 2 August 2025, whereas, following the amendments introduced by Regulation (EU) 2026/1744, certain requirements for high-risk AI systems will apply at a later date, depending on their classification [45, Art. 113]. At the same time, the Act does not apply to AI systems used exclusively for military, defence or national security purposes [45, Art. 2(3)], which is of particular importance for delineating the civilian and defence regulation of AI. The updated eIDAS framework, established by Regulation (EU) 2024/1183, provides for the European Digital Identity Wallet, with each Member State required to provide at least one such wallet to natural and legal persons in the Union [46].

An analysis of the regulatory framework reveals that economic, environmental, and information security within EU policy exist in a state of dialectical interaction characterized by a combination of synergistic effects and contradictions. This interdependence is evident in the fact that energy diversification under the REPowerEU plan simultaneously strengthens economic and environmental security; investment screening protects both critical infrastructure and media pluralism; and the cyber-defense of energy networks serves as a tool for both information and economic security. Contradictions arise, however, where the requirements of one sphere drive up costs in another: carbon pricing reduces the price competitiveness of carbon-intensive industries, while the expansion of digital infrastructure increases energy consumption. The EU addresses these contradictions through «just transition» mechanisms, the concept of the twin (green and digital) transition, and the phased implementation of requirements. For Ukraine, where wartime threats simultaneously impact all three spheres, this dialectic takes on particular urgency; a strike on energy infrastructure constitutes a threat to economic security, a source of environmental pollution, and a tool for psychological pressure on society – all at once.

A. Bradford describes the EU's capacity to extend its regulatory standards beyond the Union's borders as the "Brussels effect" [47]. For Ukraine, this means that approximation to the EU digital acquis is not only a component of the accession negotiations but also an important precondition for deeper integration into the EU internal market and for operating in a regulatory environment in which European standards exert considerable international influence. A summary of the regulatory instruments is presented in Fig. 1.3.

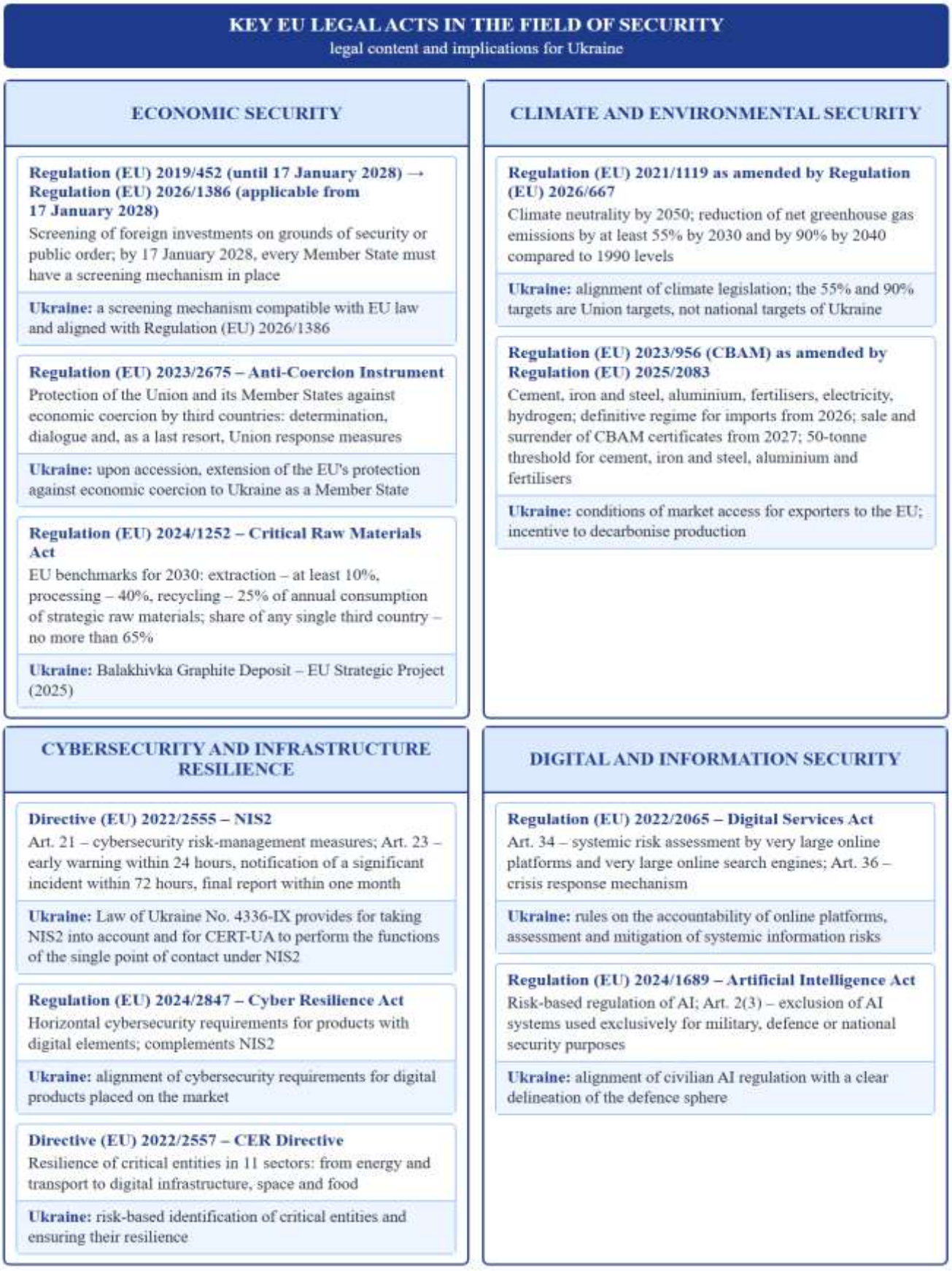


Fig. 1.3. Key EU legal acts in the fields of economic, climate, cyber, digital and infrastructure security and their implications for Ukraine

Source: compiled by the authors based on [17-19; 25-28; 30-36; 38-46; 48-51].

The synthesis of the analysis conducted above makes it possible to propose a conceptual model of the transformation of EU security policy in the context of global challenges (Fig. 1.4). The model follows the logic of "challenges – paradigm shift – strategic framework – integrated model – governance mechanism – strategic outcome" and captures the causal relationship between the nature of threats and the Union's institutional response to them. Its starting level comprises a set of military and geopolitical, hybrid and information, cyber, economic and technological, energy, climate and societal threats. What these threats have in common is their transnational and cascading nature: a shock originating in one domain rapidly spreads to others, and its consequences cannot be neutralised by the efforts of a single state. It is precisely this property, substantiated in the concept of the «risk society» [2], that necessitates a supranational level of security governance.

The EU's response to such threats has been a shift in the security paradigm, which the model depicts as a sequential transition from crisis response to prevention and deterrence, then to preparedness and resilience and, ultimately, to the capacity to adapt and recover. This transition is consistent with the understanding of resilience as a dynamic process rather than a static state [9], as well as with the concept of comprehensive preparedness set out in the report by S. Niinistö [14]. The paradigm shift has found its institutional expression in a system of strategic documents, each of which constitutes a distinct element of the strategic framework. The 2016 Global Strategy established resilience as a priority of external action [6]; the Strategic Compass transformed security policy into a programme of action structured around the pillars "Act – Secure – Invest – Partner" [16]; and the Economic Security Strategy introduced the de-risking approach [17]. The 2024 European Defence Industrial Strategy set the objective of achieving EU defence industrial readiness based on the principle of investing "more, better, together and European" [48], while the White Paper for European Defence – Readiness 2030 focused on the development of defence capabilities and defence readiness [18]. The ProtectEU strategy updated approaches to internal security, including countering hybrid threats [49], and the Preparedness Union Strategy extended the logic of preparedness to all hazards [15]. On the basis of this framework, an integrated model of European security is taking shape that combines five interrelated dimensions: defence (military capabilities, interoperability, deterrence), economic and technological (supply chain stability, critical technologies, strategic autonomy), cyber and information (cyber defence, countering disinformation), internal security (countering terrorism and crime, protection of critical infrastructure) and civilian (crisis management, whole-of-society engagement, institutional resilience). At the core of this model lies the European security space as a system within which these dimensions do not merely coexist but mutually reinforce one another.

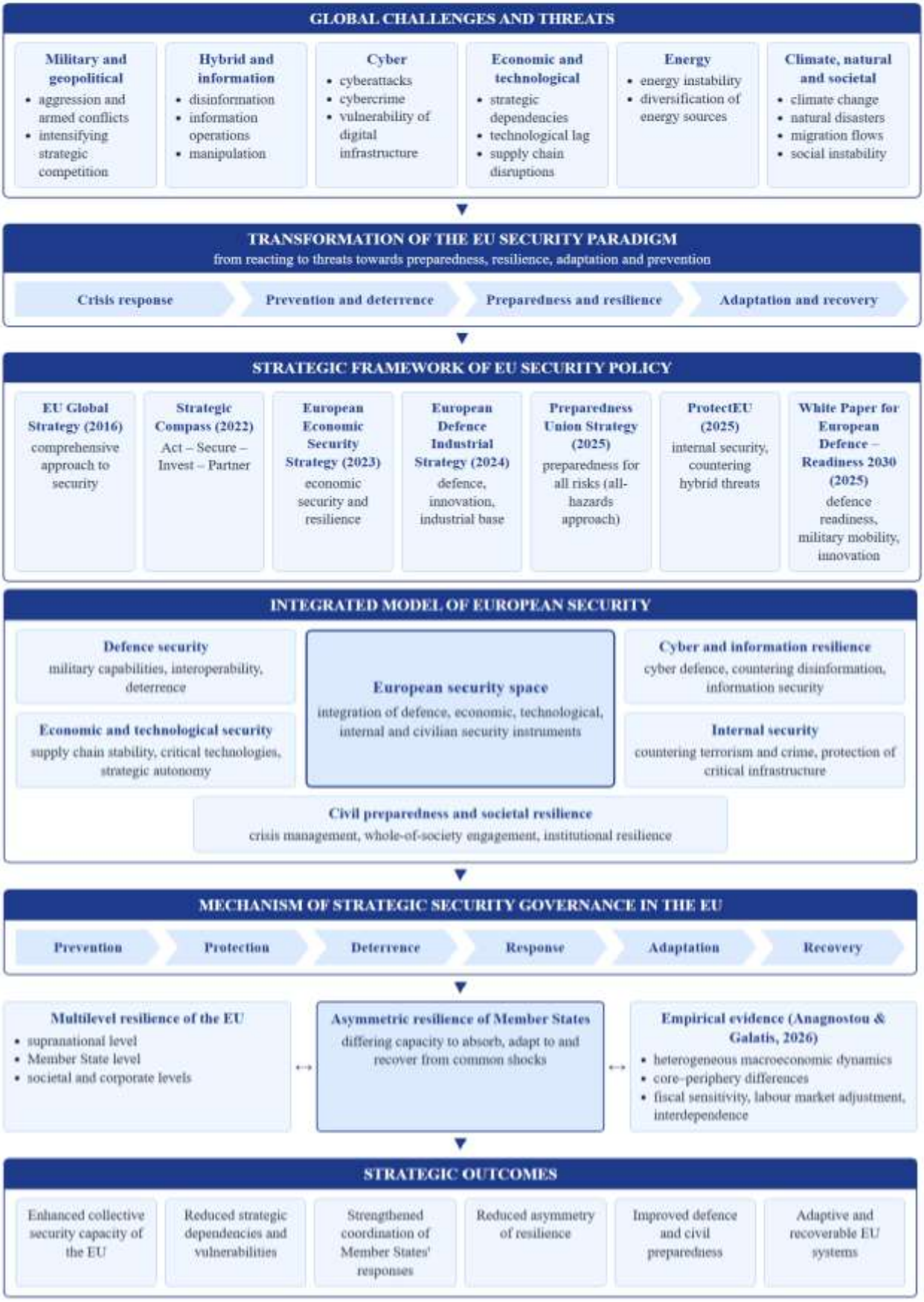


Fig. 1.4. Conceptual model of the transformation of European Union security policy in the context of global challenges

Source: developed by the authors

The proposed model has three fundamental features. First, it reflects a shift from a sectoral to an integrated understanding of security. Whereas the Copenhagen School distinguished the sectors of security as relatively autonomous objects of analysis [1], in the model they appear as interrelated dimensions of a single security space, linked by a common mechanism of strategic governance encompassing prevention, protection, deterrence, response, adaptation and recovery. Second, the model takes into account the multilevel nature of resilience, which is built simultaneously at the supranational level, at Member State level, and at the societal and corporate levels; it is precisely this whole-of-government and whole-of-society logic that underpins the report by S. Niinistö [14] and the Preparedness Union Strategy [15]. Third, the model captures the asymmetric resilience of Member States: within a common institutional framework, their capacity to absorb shocks, adapt and recover differs substantially, as empirical evidence for the euro area demonstrates [13]. Consequently, the strategic outcome of the transformation lies not only in enhancing the EU's collective security capacity, strengthening the coordination of Member States' responses and reducing strategic dependencies [17], but also in reducing the asymmetry of resilience across Member States, improving defence and civil preparedness, and ensuring the adaptability and recoverability of EU systems. For Ukraine, this conclusion has direct practical significance: integration into the European security space entails not only approximation to the EU's legal and institutional standards but also the development of its own capacities to absorb shocks and recover from them.

1.2. EU-Ukraine Partnership in the Field of Security

The legal basis of EU–Ukraine relations has evolved from a framework cooperation agreement to an agreement on political association and economic integration. The Partnership and Cooperation Agreement, signed on 14 June 1994 and in force since 1 March 1998, established the institutional mechanisms of political dialogue but did not contain a security component in the modern sense [54]. The Common Strategy of the European Council on Ukraine of 11 December 1999 recognised Ukraine's strategic importance for regional stability but did not envisage a membership perspective [55].

A qualitatively new level of contractual relations was established by the Association Agreement, the political provisions of which were signed on 21 March

2014 and the remaining provisions on 27 June 2014; the Agreement entered fully into force on 1 September 2017 [56]. Title II of the Agreement, "Political Dialogue and Reform, Political Association, Cooperation and Convergence in the Field of Foreign and Security Policy", for the first time made security a subject of treaty obligations. Article 7 provides for gradual convergence in the area of foreign and security policy, including the Common Security and Defence Policy, while Article 10 sets out cooperation in conflict prevention, crisis management and military-technological cooperation [56, Arts. 7, 10]. Title V of the Agreement, devoted to economic and sector cooperation, contains provisions on energy, the environment and the information society, which form the legal basis for the approximation of Ukrainian legislation to EU law in the fields of economic, environmental and information security.

An analysis of the history of relations demonstrates that each qualitative leap in the security partnership was triggered by an external crisis that altered the perception of risks both in Ukraine and in the EU. This provides grounds for proposing a crisis-catalytic model of the partnership's evolution, in which external shocks act as accelerators of institutional integration (Table 1.2).

Table 1.2

Evolution of the EU-Ukraine Partnership towards Security Integration

Period	Nature of the phase	External context and critical junctures	Key legal and institutional outcomes
1	2	3	4
1991-1994	Establishment of bilateral relations following Ukraine's independence	Dissolution of the USSR; emergence of Ukraine as an independent European state	Recognition of Ukraine's independence by the European Communities; signing of the Partnership and Cooperation Agreement (PCA) in 1994
1995-2003	Institutionalisation of EU–Ukraine relations	Post-Cold War institutional transformation; eastward enlargement of the EU and NATO	Entry into force of the PCA (1998); European Council Common Strategy on Ukraine (1999); development of permanent bilateral cooperation mechanisms
2004-2009	European Neighbourhood Policy and deepening political association	EU enlargement of 2004/2007; Orange Revolution; deterioration of the regional security environment after 2008	European Neighbourhood Policy; EU–Ukraine Action Plan (2005); launch of negotiations on a new enhanced agreement (2007); DCFTA negotiations (2008); Eastern Partnership (2009)
2010-2013	Preparation for association and increasing political conditionality	Regional security concerns; rule-of-law and democratic governance tensions; suspension of preparations to sign the Association Agreement and the beginning of Euromaidan in 2013	Visa Liberalisation Action Plan (2010); completion of Association Agreement negotiations (2011); initialling of the Association Agreement and DCFTA (2012)

1	2	3	4
2014-2021	Association and security cooperation under Russian aggression	Illegal annexation of Crimea by Russia; armed conflict in eastern Ukraine	Signing of the Association Agreement (2014); EU restrictive measures against Russia; establishment of EUAM Ukraine (2014); provisional application of the DCFTA (2016); full entry into force of the Association Agreement and visa-free regime (2017)
Since 2022	Accession process and deepened security integration	Russia's full-scale invasion of Ukraine	EU candidate status (2022); establishment of EUMAM Ukraine (2022); opening of accession negotiations (2024); Joint Security Commitments (2024); Ukraine Facility (2024); opening of Cluster 1 «Fundamentals» and Cluster 6 «External Relations» in 2026

Source: compiled by the authors based on [23; 54-57].

An analysis of the data in the table indicates that the first two phases (1991–2003) were predominantly declaratory and institutional in nature. The 1994 Partnership and Cooperation Agreement established mechanisms of political dialogue, yet the security component of relations was limited to nuclear disarmament and regional stability [54]. The 1999 Common Strategy of the European Council recognised Ukraine's strategic importance but did not envisage a membership perspective [55], and the EU perceived Ukraine primarily through the lens of the post-Soviet space. The eastward enlargement of the EU and NATO, which served as the catalysing crisis of the second phase, simultaneously opened up new opportunities for Ukraine and heightened the risk of its ending up in a «grey zone» of European security. The third and fourth phases (2004–2013) marked a shift from general dialogue to a concrete association agenda: the Orange Revolution demonstrated the European orientation of Ukrainian society, and Ukraine was included in the European Neighbourhood Policy and the Eastern Partnership. The Russo-Georgian War of 2008 demonstrated, for the first time since the end of the Cold War, Russia's readiness to use military force against its neighbours. Nevertheless, the security dimension of relations during this period remained potential rather than practical.

The fifth phase (2014–2021) proved to be a turning point, as the annexation of Crimea and the armed aggression in Donbas transformed Ukraine's security from a

peripheral issue into one of the priorities of European policy. The Association Agreement for the first time enshrined security as a subject of treaty obligations [56], while the visa-free regime, sectoral sanctions against Russia and the EU Advisory Mission Ukraine marked a transition from a neighbourhood policy to a policy of strategic support. The sixth phase, which began with the full-scale invasion on 24 February 2022, is characterised by unprecedented rapprochement. Within a few months, Ukraine's power system was synchronised with the Continental European grid, Ukraine was granted candidate status, and accession negotiations were opened in June 2024. In parallel, a system of long-term instruments was established, including the Joint Security Commitments [23] and the Ukraine Facility [57]. Thus, over three decades, the nature of the partnership has evolved from declaratory dialogue to integration, within which Ukraine's security is increasingly regarded as a component of the security of the Union itself.

The evolution outlined above allows us to characterise it as a crisis-catalytic model, which has both a positive and a problematic dimension. The positive dimension is that each crisis opened a «window of opportunity» for institutional breakthroughs that would otherwise have required considerably more time. The problematic dimension relates to the reactive nature of the model: integration proceeded as a response to threats rather than as a result of deliberate strategic planning by both sides. It is precisely this reactivity that explains the persistent gap between declared ambitions and the practical substance of security cooperation until 2022, and that makes the transition to a proactive model of partnership a key task of the current stage.

Russia's full-scale invasion led to the formation of an unprecedented and increasingly institutionalised system of EU support for Ukraine. Its distinguishing feature is the combination of military assistance with defence-industrial cooperation, macro-financial support, energy and cyber resilience, restrictive measures against Russia, and instruments aimed at strengthening Ukraine's long-term economic and technological security. The Joint Security Commitments of 27 June 2024 consolidated this comprehensive approach by explicitly linking military assistance, resilience, macro-financial support, reconstruction, reforms and wider security commitments [67].

The instruments summarised in Table 1.3 reveal a clear evolution in the logic of EU support. The measures adopted in 2022 were predominantly of an emergency nature and aimed at ensuring Ukraine's immediate survival and resilience: military assistance and training under the European Peace Facility and EUMAM Ukraine [58; 59], the emergency synchronisation of the power system [70], energy and civil protection assistance [71; 72], and the expansion of restrictive measures against Russia [73–76].

Table 1.3

Key Instruments of EU Security Support for Ukraine since 2022

Dimension	**Instrument**	**Legal / institutional basis**	**Main content**
1	2	3	4
Military	European Peace Facility (EPF) / Ukraine Assistance Fund	Council Decision (CFSP) 2021/509 [58], as amended	Financing of lethal and non-lethal military equipment and training. In March 2024, a dedicated Ukraine Assistance Fund of EUR 5 billion was established within the EPF.
Military	EU Military Assistance Mission in support of Ukraine	Council Decision (CFSP) 2022/1968 [59], as amended	Individual, collective and specialised training of personnel of the Armed Forces of Ukraine aimed at strengthening their military capability and resilience.
Defence-industrial	SAFE – Security Action for Europe	Council Regulation (EU) 2025/1106 [22]	Provides up to EUR 150 billion in loans to EU Member States for defence investment through common procurement. Ukraine is included in the eligibility framework for common procurement, while Ukrainian defence companies may participate in relevant supply chains.
Defence-industrial	EDIP – Ukraine Support Instrument	Regulation (EU) 2025/2643 [68]	A dedicated cooperation instrument for the recovery, reconstruction and modernisation of the Ukrainian Defence Technological and Industrial Base (Ukrainian DTIB), taking into account its possible future integration into the EDTIB. The financial envelope for 30 December 2025–31 December 2027 amounts to EUR 300 million, supplemented by possible additional contributions.
Political and security	Joint Security Commitments between the EU and Ukraine	Joint Security Commitments of 27 June 2024 [23]	Long-term support aimed at strengthening Ukraine's capacity to defend itself, resist destabilisation and deter future aggression; covers military, defence-industrial, cyber, hybrid, economic and broader resilience dimensions.
Financial and economic	Ukraine Facility	Regulation (EU) 2024/792 [57]	Up to EUR 50 billion for 2024–2027 in loans and non-repayable support for macro-financial stability, recovery, reconstruction, modernisation, investment and reforms linked to Ukraine's EU accession path.
Cyber	EU Cybersecurity Reserve	Regulation (EU) 2025/38; Council Implementing Decision (EU) 2026/1354 [69]	Regulation (EU) 2025/38 establishes the EU Cybersecurity Reserve; Decision (EU) 2026/1354 specifically authorises the provision of support from the Reserve to Ukraine in response to significant and large-scale-equivalent cybersecurity incidents. The authorisation applies until 17 June 2027.

1	2	3	4
Energy	Emergency synchronisation with the Continental European power system	Decision of the Continental Europe transmission system operators, 16 March 2022 [70]	Emergency synchronisation of the Ukrainian and Moldovan power systems with Continental Europe, strengthening the stability of Ukraine's electricity system and its integration with the European grid.
Energy / resilience	Ukraine Energy Support Fund	Institutional framework established by the Energy Community Secretariat in 2022 at the request of the European Commission and in agreement with the Ministry of Energy of Ukraine [71]	Mobilisation of financial resources for equipment, spare parts and services required to restore and maintain the functioning of Ukraine's energy infrastructure.
Civil protection / resilience	Union Civil Protection Mechanism (UCPM)	Decision No 1313/2013/EU of the European Parliament and of the Council, as amended [72]	Framework for coordinated civil-protection assistance, including emergency equipment, generators, medical assistance and other in-kind support provided to Ukraine.
Sanctions / economic security	EU restrictive measures against Russia – sectoral regime	Council Decision 2014/512/CFSP; Council Regulation (EU) No 833/2014, as amended [73]	Sectoral economic restrictive measures covering, inter alia, trade, finance, energy, technology and dual-use goods, aimed at constraining Russia's capacity to sustain its aggression against Ukraine.
Sanctions / economic security	EU restrictive measures against Russia – individual regime	Council Decision 2014/145/CFSP; Council Regulation (EU) No 269/2014, as amended [76]	Asset freezes and related individual restrictive measures against persons and entities responsible for actions undermining or threatening Ukraine's territorial integrity, sovereignty and independence.
Economic resilience / critical raw materials	EU–Ukraine Strategic Partnership on Raw Materials and Batteries	Memorandum of Understanding of 13 July 2021 [29]; Commission Decision (EU) 2025/1174 [60]	Integration of Ukrainian critical-raw-material and battery value chains with the EU; diversification and strengthening of supply security. In 2025, the Balakhivka Graphite Deposit in Ukraine was recognised as an EU Strategic Project under the Critical Raw Materials Act.

Source: compiled by the authors based on [22; 29; 41; 57–60; 67–76].

From 2024 onwards, the emphasis shifted towards long-term and structurally embedded instruments: the Ukraine Facility links financial support to reforms under the Ukraine Plan [57], while SAFE and the EDIP Ukraine Support Instrument open the way for Ukraine's defence industry to participate in European procurement and supply chains, with a view to its possible future integration into the EDTIB [22; 68]. The authorisation of support from the EU Cybersecurity Reserve [41; 69] and the recognition of a Ukrainian raw materials project as an EU Strategic Project [60] further indicate that Ukraine is being incorporated into specific EU mechanisms ahead of formal accession. The legal bases of these instruments are notably heterogeneous, ranging from CFSP decisions and EU regulations to non-binding political commitments and institutional frameworks managed by international organisations. In our view, this reflects a transition in Ukraine's status from a recipient of emergency assistance to a partner progressively integrated into the EU's security, defence-industrial and resilience architecture, a process that may be characterised as pre-accession security integration.

Of the instruments listed in Table 1.3, the Joint Security Commitments, the Ukraine Facility, the energy synchronisation and Ukraine's access to the EU Cybersecurity Reserve merit separate analysis.

The Joint Security Commitments between the EU and Ukraine of 27 June 2024 [67] set out the areas of long-term support, including military assistance, training of military personnel, development of the defence industry, demining, cybersecurity, countering hybrid threats, sanctions pressure on the aggressor and accountability. Of fundamental importance is the mechanism they provide for consultations on Ukraine's needs in the event of future aggression. Although the commitments are not legally binding and do not constitute collective defence guarantees within the meaning of Article 42(7) TEU [3], they institutionalise the security partnership for the period until Ukraine's accession to the EU.

The Ukraine Facility, established by Regulation (EU) 2024/792 [57], embodies a fundamentally new approach to financial support: funds are disbursed subject to the achievement of defined reform milestones set out in the Ukraine Plan. The Facility comprises three pillars: support to the state budget based on the Ukraine Plan, the Ukraine Investment Framework for mobilising private investment, and Union support measures. As a result, financial support is directly linked to approximation to European standards, and the Facility itself becomes an instrument not only of recovery but also of integration.

The energy synchronisation deserves particular attention as an example of a security function being fulfilled through technical integration. The project to synchronise the power systems of Ukraine and Moldova with the Continental European power system had been under way since 2017 and involved the implementation of a

set of technical measures. Following a request from Ukrenergo and Moldelectrica in late February 2022, the Continental Europe transmission system operators agreed to an emergency synchronisation, which was completed on 16 March 2022 [70]. The synchronisation simultaneously eliminated the dependence of Ukraine's power system on the Russian-Belarusian grid, made it possible to import electricity from the EU amid massive strikes on generation capacity, and created the preconditions for integration into the European energy market. The restoration of damaged infrastructure is supported by the Ukraine Energy Support Fund, managed by the Energy Community Secretariat [71]; Ukraine has been a Contracting Party to the Energy Community since 2011.

In the field of cybersecurity, cooperation has acquired a practical character. In addition to the exchange of threat information, its foundation has been Ukraine's association with the Digital Europe Programme. It was this association that provided the legal basis for the Council decision of 15 June 2026 authorising the provision of support to Ukraine from the EU Cybersecurity Reserve established by the Cyber Solidarity Act [41; 69]. Ukraine is now able to receive incident response services from trusted European providers in the event of significant or large-scale cybersecurity incidents. This marks a shift from information exchange to direct operational support from the Union.

1.3. Roadmap for Ukraine's integration into the European security space

The design of a roadmap for Ukraine's integration into the European security space must take into account two frameworks that determine its content and logic. The first is the accession negotiating framework. Under Article 49 TEU, any European State which respects the values referred to in Article 2 and is committed to promoting them may apply to become a member of the Union [3, Art. 49]. Ukraine submitted its application on 28 February 2022, was granted candidate status on 23 June 2022, and the first intergovernmental conference formally opening accession negotiations was held on 25 June 2024. The negotiations are conducted under the revised enlargement methodology of 2020, which groups the negotiating chapters into six thematic clusters and applies the "fundamentals first" principle [77]. For the subject of this study, the most relevant are the Fundamentals cluster (in particular Chapter 24 "Justice, freedom and security"), the Internal Market cluster (in particular Chapter 4 "Free movement of

capital", which is relevant to foreign investment screening), the Competitiveness and inclusive growth cluster (Chapter 10 "Digital transformation and media" and Chapter 20 "Enterprise and industrial policy"), the Green agenda and sustainable connectivity cluster (Chapter 15 «Energy» and Chapter 27 "Environment and climate change"), and the External relations cluster (Chapter 30 "External relations" and Chapter 31 "Foreign, security and defence policy").

The second framework is formed by the conditions under which integration takes place. European security models were developed under conditions of relative stability, whereas Ukraine is implementing them amid war, large-scale destruction and resource constraints. A mechanical transfer of European practices under such conditions is not feasible, while abandoning them would contradict the strategic goal of membership. In our view, this contradiction can be resolved through adaptive implementation, which implies preserving the substance of European standards while allowing flexibility in the forms, pace and sequencing of their implementation (Fig. 1.4).

Adaptive implementation rests on several interrelated principles. First, European standards are reinterpreted in the light of wartime realities without abandoning their underlying values. Second, economic, environmental and information security are treated as a single system, in which decisions in one domain are assessed in terms of their consequences for the others. Third, the process is divided into stages with clear objectives and completion criteria synchronised with the negotiating clusters. Fourth, priority is given to systems capable of functioning under partial destruction and of recovering rapidly. Fifth, Ukraine's experience in countering hybrid threats is recognised as a resource that may be ahead of European practice and should be institutionalised within common mechanisms. Sixth, limited resources are channelled into measures that simultaneously strengthen several dimensions of security.

It is important to distinguish adaptive implementation from selective or deferred approximation. Adaptability concerns not whether a standard should be implemented, but how and in what sequence. Thus, the Artificial Intelligence Act does not apply to AI systems used exclusively for military, defence or national security purposes [45, Art. 2(3)]; a state at war has good grounds to make full use of this exclusion while implementing the requirements for civilian uses of AI. Similarly, the NIS2 Directive sets minimum harmonisation requirements [38], which allows Ukraine to introduce stricter national cyber defence rules justified by the level of threats. Adaptability also means orientation towards the current state of the acquis: in the field of investment screening, it is advisable to take into account from the outset the requirements of Regulation (EU) 2026/1386, which will apply from 17 January 2028 and replace Regulation (EU) 2019/452 [25; 78].

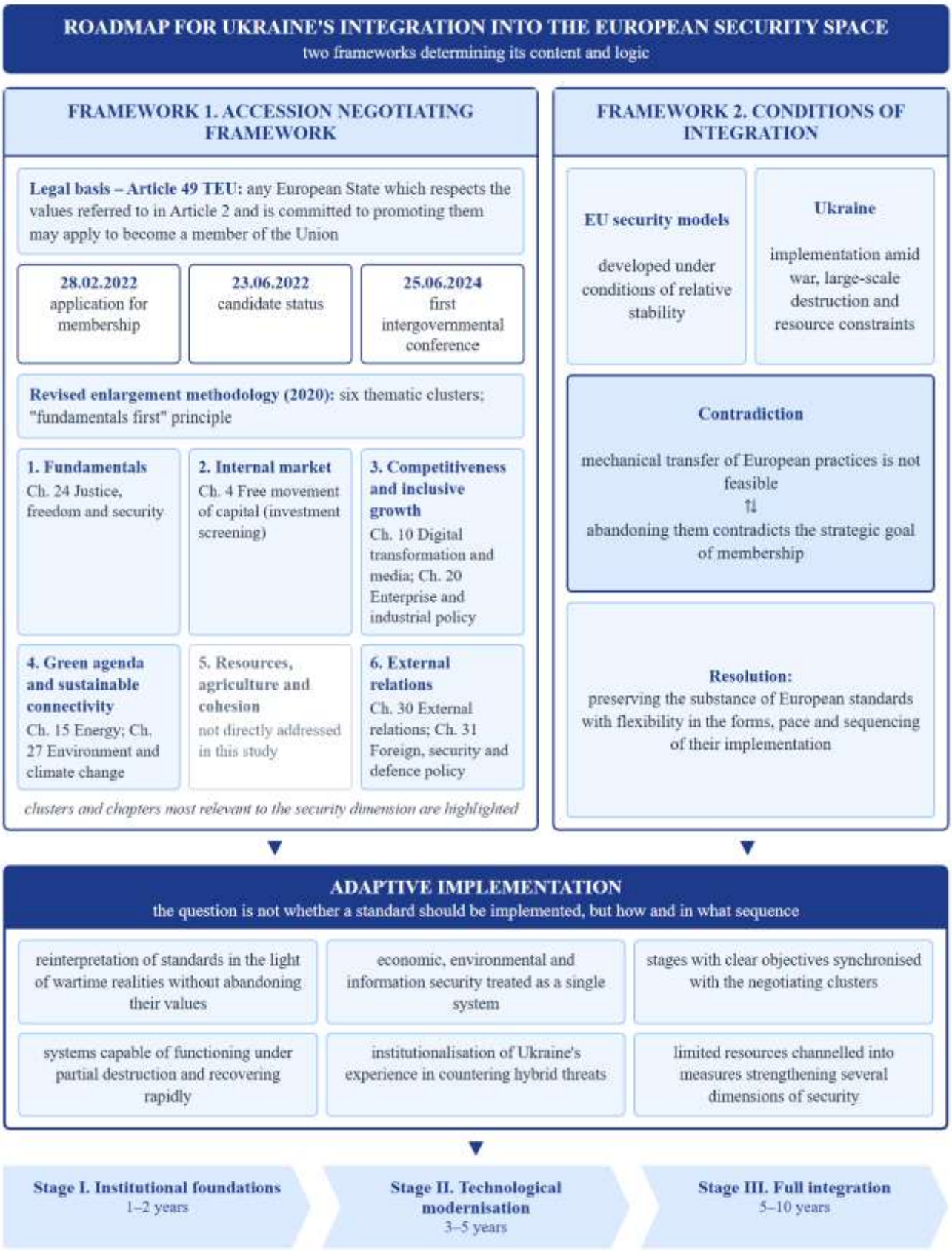


Fig. 1.4. Decomposition of the roadmap for Ukraine's integration into the European security space

Source: developed by the authors based on [3; 77].

In accordance with the foundations outlined above, the roadmap comprises three stages, for each of which priorities in the economic, environmental and information domains, the relevant negotiating chapters and the EU acts to be approximated are identified (Table 1.4).

Table 1.4

Roadmap for Ukraine's Integration into the European Security Space

Stage	Domain	Negotiating chapters	EU benchmarks	Priority tasks
I. Institutional foundations (1–2 years)	Economic	4, 20, 30	Economic Security Strategy [17]; Regulations (EU) 2019/452 [25] and 2026/1386 [78]	Adoption of a new Economic Security Strategy of Ukraine incorporating the de-risking approach; establishment of a foreign investment screening mechanism compatible with Regulation (EU) 2026/1386
	Environmental	15, 27	Regulation (EU) 2021/1119 [31] as amended by Regulation (EU) 2026/667 [33]	Approximation of climate legislation; system for documenting and assessing environmental damage caused by the war
	Information	10, 24	NIS2 [38] and CER [39] Directives; GDPR [42]	Completion of NIS2 approximation initiated by Law No. 4336-IX [66]; approximation of critical infrastructure legislation; updating of personal data protection legislation
II. Technological modernisation (3–5 years)	Economic	20, 30	Regulations (EU) 2024/1252 [28] and 2023/1781 [27]; SAFE [22]; EDIP [68]	Development of strategic raw material projects, including those recognised by the EU [60]; participation in European defence procurement and supply chains
	Environmental	15, 27	REPowerEU [32]; RED III [34]; Regulation (EU) 2023/956 [35] as amended by Regulation (EU) 2025/2083 [79]	Decentralised renewable-based energy; integration into the EU energy market; adaptation of metallurgy, fertiliser production and other CBAM-covered industries
	Information	10	eIDAS [46]; DSA [43]; AI Act [45]; CRA [40]	Compatibility of electronic identification systems; risk-based regulation of civilian AI; online platform accountability rules; cybersecurity requirements for digital products
III. Full integration (5–10 years)	All domains	31 and others	Strategic Compass [16]; Preparedness Union Strategy [15]	Participation in EU economic security instruments, the Emissions Trading System and cybersecurity mechanisms as a Member State; institutionalisation of Ukraine's security experience within common mechanisms

The first stage aims to lay the institutional foundations. Its central task is the renewal of strategic documents, above all the Economic Security Strategy of Ukraine, whose term expired in 2025 without a successor strategy having been adopted as of September 2026 [63]. A new strategy should reproduce the three-pillar logic of the European strategy ("promoting – protecting – partnering") and its risk classification [17], thereby ensuring methodological compatibility between national and European policies. In the information domain, this stage builds on processes already under way: Law No. 4336-IX initiated the approximation of Ukrainian legislation to NIS2 [66], and the Cybersecurity Strategy of Ukraine is implemented through annual action plans, the most recent of which was approved in June 2026 [51]. In parallel, it is necessary to establish an interagency coordination mechanism capable of assessing security decisions in terms of their consequences for all three domains and to synchronise legislative changes with the logic of the negotiating clusters.

The second stage covers technological modernisation. In the economic domain, the priority is to transform Ukraine from a supplier of raw materials into a participant in European value chains. The first steps have already been taken: the Balakhivka graphite deposit has been recognised as an EU Strategic Project under the Critical Raw Materials Act [60], while SAFE and the EDIP Ukraine Support Instrument open opportunities for Ukraine's defence industry to participate in European procurement and supply chains, with a view to its possible future integration into the EDTIB [22; 68]. In the environmental domain, the greatest synergy is offered by decentralised renewable-based energy, which simultaneously increases the resilience of the power system to military strikes, reduces emissions and is consistent with the objectives of the revised Renewable Energy Directive [34]. Particular attention should be paid to adapting export-oriented industries to CBAM, whose definitive regime applies to imports from 2026, with the sale and surrender of CBAM certificates starting in 2027 [35; 79]. In the information domain, the priorities are the compatibility of national digital services with the European Digital Identity Wallet [46], the implementation of the requirements of the Artificial Intelligence Act and the Cyber Resilience Act [45; 40], and the effective use of the EU Cybersecurity Reserve, to which Ukraine has been granted access [69].

The third stage envisages full integration, in which Ukraine participates in the EU's common security mechanisms as a Member State, including the mutual assistance clause under Article 42(7) TEU [3]. In our view, its core should be the institutionalisation of Ukraine's security experience, which transforms the very logic of integration from one-sided adaptation to mutual learning.

The implementation of the roadmap faces a number of risks, which can be grouped by source. Resource risks stem from the concentration of budgetary funds on defence needs, which limits the financing of reforms; they can be mitigated by

combining budgetary resources with EU instruments, above all the Ukraine Facility, and by mobilising private capital through the Ukraine Investment Framework [57]. Human capital risks relate to losses caused by migration and mobilisation, which are particularly acute in engineering and digital professions. Institutional risks consist in the instability of management teams and the fragmentation of competences among agencies. Political risks concern the pace of the negotiating process, since the opening of clusters requires unanimous decisions of the Member States. Regional risks arise from the uneven consequences of the war, which call for a differentiated approach to frontline, de-occupied and rear regions. A separate risk is the dynamic nature of the acquis itself: the updating of EU acts in 2025–2026, including the new Regulation on foreign investment screening, the 2040 climate target and the simplification of CBAM [78; 33; 79], requires continuous monitoring of changes and adjustment of national approximation plans.

The effectiveness of the roadmap depends on a monitoring system that reflects not only formal compliance with EU norms but also the actual resilience of national security systems. In designing it, account should be taken of the methodological conclusion that the existence of equilibrium-restoration mechanisms does not in itself demonstrate resilience; what matters is the speed, coordination and persistence of the adjustment process [13]. In line with the understanding of resilience as a dynamic process [9], the monitoring system should combine static compliance indicators with dynamic indicators reflecting the speed with which key macroeconomic variables (GDP, inflation, public debt and unemployment) return to their equilibrium path after shocks. The experience of the peripheral euro-area economies, characterised by prolonged fiscal and labour market adjustment after shocks [13], is particularly instructive for Ukraine in view of the growth of public debt and the loss of human capital caused by the war. The proposed system of indicators is presented in Table 1.5.

Table 1.5

System of Indicators for Monitoring the Implementation of the Roadmap

Domain	Indicator	EU benchmark	Data source
1	2	3	4
General	Level of preparation under negotiating chapters 4, 10, 15, 20, 24, 27 and 31	"Good level of preparation" or higher	European Commission's annual report on Ukraine
Macroeconomic	Duration of deviations of GDP, inflation, public debt and unemployment from the equilibrium path after a shock	Comparison with Member States' adjustment trajectories [13]	State Statistics Service of Ukraine, National Bank of Ukraine, Ministry of Finance of Ukraine, Eurostat
Economic	Share of the largest external supplier in imports of critical raw materials	Not more than 65% [28]	State Statistics Service of Ukraine, Eurostat

1	2	3	4
Economic	Existence and coverage of a foreign investment screening mechanism	Compatibility with Regulation (EU) 2026/1386 [78]	Legislative monitoring
Environmental	Share of renewable energy in gross final energy consumption	42.5% by 2030 in the EU [34]	Energy Community, State Statistics Service of Ukraine
Environmental	Carbon intensity of exports of CBAM-covered goods	Competitiveness under CBAM [35; 79]	Sectoral reporting
Information	Share of persons aged 16–74 with at least basic digital skills	80% [37]	Ministry of Digital Transformation of Ukraine, State Statistics Service of Ukraine
Information	Timeliness of notification of significant cyber incidents	24 hours (early warning) / 72 hours (incident notification) [38]	CERT-UA
Information	Share of key public services available online	100% [37]	Ministry of Digital Transformation of Ukraine

The proposed system of indicators has three methodological advantages. First, it links national indicators to quantitative benchmarks enshrined in EU legal acts, ensuring comparability and allowing the use of European data sources. Second, the combination of compliance and performance indicators makes it possible to avoid a situation in which formal legislative approximation is not accompanied by a genuine strengthening of resilience. Third, the inclusion of dynamic macroeconomic indicators makes it possible to assess not only the level but also the process of the national economy's adjustment to shocks, comparing it with the trajectories of the Member States.

The analysis conducted in this chapter shows that the EU's security policy has undergone a profound conceptual and institutional transformation, evolving from crisis management towards strategic resilience and comprehensive preparedness. The theoretical foundations of this evolution were laid by the broadened understanding of security developed by the Copenhagen School and by the concept of the «risk society», which explain why threats of a non-military, transnational and cascading nature have become the subject of security policy. The legal basis of EU security policy is formed by the provisions of the founding Treaties, in particular Articles 21 and 42 TEU and Article 222 TFEU, which combine a defence dimension related to armed aggression with a resilience dimension related to non-military threats. The central concept of this transformation is resilience, which was introduced by the 2016 Global Strategy and subsequently acquired concrete instrumental content in the EU's strategic documents and legal acts of the 2020s. On this basis, we propose to understand the European

security space as a multilevel institutional and normative system within which the Member States, EU institutions and associated partners coordinate policies of prevention, deterrence, mitigation and recovery from threats in the military, economic, environmental, information and social domains on the basis of shared values and rules.

The Strategic Compass of 2022 transformed EU security policy into a programme of action with the stated objective of making the EU a stronger and more capable security provider, while the Economic Security Strategy of 2023 introduced the de-risking approach as the methodological basis for managing economic risks. A distinctive feature of the EU as a security actor is that a significant part of its security policy is implemented through the regulation of the internal market, energy, the environment and the digital economy. The analysis of the relevant legal acts, including the recent updating of the acquis in 2025–2026, has revealed the dialectical nature of the interaction between economic, environmental and information security, which combines synergistic effects with contradictions. The conceptual model of the transformation of EU security policy proposed in the chapter integrates these findings and shows that resilience within the Union is multilevel and asymmetric: under a common institutional framework, the capacity of Member States to absorb shocks, adapt and recover differs substantially.

The study of the EU–Ukraine partnership in the field of security has made it possible to identify six phases in its evolution, each of which was triggered by an external crisis, and to substantiate the crisis-catalytic model of integration. After 2022, EU support for Ukraine developed from emergency assistance into an increasingly institutionalised system combining military, defence-industrial, financial, energy, cyber, civil protection and sanctions instruments. The inclusion of Ukraine in specific EU mechanisms ahead of formal accession, in particular in the field of defence procurement, critical raw materials and cybersecurity, allows this process to be characterised as pre-accession security integration. At the same time, a comparison of Ukraine's national security policy with EU approaches has revealed temporal, conceptual and instrumental discrepancies, the most significant of which is the absence of a new Economic Security Strategy of Ukraine after the expiry of the previous one in 2025. In a number of areas, however, Ukrainian practice is ahead of European practice, which creates the preconditions for moving from a reactive to a proactive model of partnership in which Ukraine acts as a co-creator of the common security space.

The roadmap for Ukraine's integration into the European security space developed in the chapter is based on the concept of adaptive implementation, which implies preserving the substance of European standards while allowing flexibility in the forms, pace and sequencing of their implementation, as well as orientation towards the current state of the acquis. The roadmap is synchronised with the accession

negotiating clusters and chapters and comprises three stages – institutional foundations, technological modernisation and full integration with priorities defined for the economic, environmental and information domains. The proposed monitoring system combines static indicators of compliance with EU legal benchmarks with dynamic indicators of macroeconomic resilience, which makes it possible to assess not only the formal approximation of legislation but also the actual capacity of Ukraine's security systems to withstand and recover from shocks.

References

1. Buzan B., Waever O., de Wilde J. Security: A new framework for analysis. Boulder : Lynne Rienner, 1998. 239 p. ISBN 978-1-55587-784-2.

2. Beck U. Risk society: Towards a new modernity. London : Sage, 1992. 260 p. ISBN 978-0-8039-8346-5.

3. European Union. (2016). Consolidated version of the Treaty on European Union. Official Journal of the European Union, C 202, 7 June 2016, pp. 13–45. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016 (accessed: 25.08.2026).

4. United Nations. (1945). Charter of the United Nations. San Francisco, 26 June 1945. Article 51. URL: https://legal.un.org/repertory/art51.shtml (accessed: 25.08.2026).

5. European Union. (2016). *Consolidated version of the Treaty on the Functioning of the European Union.* Official Journal of the European Union, C 202, 7 June 2016, Article 222, p. 148. URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2016/art_222/oj/eng?utm (accessed: 25.08.2026).

6. European Union. Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy. Brussels, 2016. URL: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf (accessed: 25.08.2026).

7. Juncos A. E. Resilience as the new EU foreign policy paradigm: A pragmatist turn? European Security. 2017. Vol. 26, No. 1. P. 1–18. DOI: https://doi.org/10.1080/09662839.2016.1247809. (accessed: 28.08.2026).

8. Wagner W., Anholt R. Resilience as the EU Global Strategy's new leitmotif: Pragmatic, problematic or promising? Contemporary Security Policy. 2016. Vol. 37, No. 3. P. 414–430. DOI: https://doi.org/10.1080/13523260.2016.1228034. (accessed: 28.08.2026).

9. Martin R., Sunley P. On the notion of regional economic resilience: Conceptualization and explanation. Journal of Economic Geography. 2015. Vol. 15, No. 1. P. 1–42. DOI: https://doi.org/10.1093/jeg/lbu015. (accessed: 28.08.2026).

10. European Commission. 2020 Strategic Foresight Report: Charting the course towards a more resilient Europe. COM(2020) 493 final. Brussels, 9/9/2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0493 (access date: 29.08.2026).

11. European Commission. EU Security Union Strategy. COM(2020) 605 final. Brussels, 24.7.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605 (accessed: 29.08.2026).

12. European Council. Informal meeting of the Heads of State or Government: Versailles Declaration. 10-11 March 2022. URL: https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf (date of access: 29.08.2026).

13. Anagnostou A., Galatis N. M. Economic resilience to inflationary and geopolitical shocks in the euro area: A comparative macroeconomic analysis. Economies. 2026. Vol. 14, No. 7. Art. 284. DOI: https://doi.org/10.3390/economies14070284.

14. Niinistö S. Safer together: Strengthening Europe's civilian and military preparedness and readiness. Brussels : European Commission, 2024.

15. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication on the European Preparedness Union Strategy. JOIN(2025) 130 final.

Brussels, 26.3.2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 52025JC0130 (дата звернення: 29.08.2026).

16. Council of the European Union. A Strategic Compass for Security and Defence. Doc. 7371/22. Brussels, 21 March 2022. URL: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf (accessed: 29.08.2026).

17. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Joint Communication on «European Economic Security Strategy». JOIN(2023) 20 final. Brussels, 20.6.2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 52023JC0020 (accessed: 29.08.2026).

18. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. Joint White Paper for European Defence Readiness 2030. JOIN(2025) 120 final. Brussels, 19.3.2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025JC0120 (accessed: 29.08.2026).

19. Council of the European Union. Council Conclusions on a Framework for a Coordinated EU Response to Hybrid Campaigns. Brussels, 21.6.2022. URL: https://www.consilium.europa.eu/en/press/press-releases/2022/06/21/council-conclusions-on-a-framework-for-a-coordinated-eu-response-to-hybrid-campaigns (accessed: 29.08.2026).

20. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. EU Policy on Cyber Defence. JOIN(2022) 49 final. Brussels, 10.11.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022JC0049&utm (accessed: 31.08.2026).

21. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. European Union Space Strategy for Security and Defence. JOIN(2023) 9 final. Brussels, 10.3.2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023JC0009&utm (accessed: 29.08.2026).

22. Council Regulation (EU) 2025/1106 of 27 May 2025 establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument. URL: https://eur-lex.europa.eu/eli/reg/2025/1106/oj (accessed: 31.08.2026).

23. European Union, Ukraine. Joint security commitments between the European Union and Ukraine. Brussels, 27 June 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/06/27/joint-security-commitments-between-the-european-union-and-ukraine (accessed: 31.08.2026).

24. Commission Recommendation (EU) 2023/2113 of 3 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States. URL: https://eur-lex.europa.eu/eli/reco/2023/2113/oj (accessed: 31.08.2026).

25. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. URL: https://eur-lex.europa.eu/eli/reg/2019/452/oj (accessed: 31.08.2026).

26. Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member States from economic coercion by third countries. URL: https://eur-lex.europa.eu/eli/reg/2023/2675/oj (accessed: 31.08.2026).

27. Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act). URL: https://eur-lex.europa.eu/eli/reg/2023/1781/oj (accessed: 31.08.2026).

28. Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024 establishing a framework for ensuring a secure and sustainable supply of critical raw materials (Critical Raw Materials Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1252/oj (accessed: 31.08.2026).

29. European Union, Ukraine. Memorandum of Understanding on a Strategic Partnership on Raw Materials, Batteries and Renewable Hydrogen. 13 July 2021.

30. European Commission. The European Green Deal. COM(2019) 640 final. Brussels, 11.12.2019. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0640 (accessed: 31.08.2026).

31. Regulation (EU) 2021/1119 of the European Parliament and of the Council of 30 June 2021 establishing the framework for achieving climate neutrality (European Climate Law). URL: https://eur-lex.europa.eu/eli/reg/2021/1119/oj (accessed: 31.08.2026).

32. European Commission. REPowerEU Plan. COM(2022) 230 final. Brussels, 18.5.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0230 (accessed: 31.08.2026).

33. Regulation (EU) 2026/667 of the European Parliament and of the Council of 11 March 2026 amending Regulation (EU) 2021/1119 as regards the setting of a Union intermediate climate target for 2040. URL: https://eur-lex.europa.eu/eli/reg/2026/667/oj (accessed: 31.08.2026).

34. Directive (EU) 2023/2413 of the European Parliament and of the Council of 18 October 2023 amending Directive (EU) 2018/2001 as regards the promotion of energy from renewable sources. URL: https://eur-lex.europa.eu/eli/dir/2023/2413/oj (accessed: 31.08.2026).

35. Regulation (EU) 2023/956 of the European Parliament and of the Council of 10 May 2023 establishing a carbon border adjustment mechanism. URL: https://eur-lex.europa.eu/eli/reg/2023/956/oj (accessed: 31.08.2026).

36. European Commission. 2030 Digital Compass: The European way for the Digital Decade. COM(2021) 118 final. Brussels, 9.3.2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0118 (accessed: 31.08.2026).

37. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030. URL: https://eur-lex.europa.eu/eli/dec/2022/2481/oj (accessed: 3.09.2026).

38. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed: 31.08.2026).

39. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed: 3.09.2026).

40. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). URL: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (accessed: 3.09.2026).

41. Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 (Cyber Solidarity Act). URL: https://eur-lex.europa.eu/eli/reg/2025/38/oj (accessed: 3.09.2026).

42. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 3.09.2026).

43. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act). URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj (accessed: 3.09.2026).

44. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (accessed: 3.09.2026).

45. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed: 3.09.2026).

46. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj (accessed: 3.09.2026).

47. Bradford A. The Brussels effect: How the European Union rules the world. New York : Oxford University Press, 2020. DOI: https://doi.org/10.1093/oso/9780190088583.001.0001.

48. On Critical Infrastructure: Law of Ukraine No. 1882-IX dated November 16, 2021 (as amended). URL: https://zakon.rada.gov.ua/laws/show/1882-20 (accessed: 7.09.2026).

49. On National Security of Ukraine: Law of Ukraine No. 2469-VIII dated June 21, 2018 (as amended). URL: https://zakon.rada.gov.ua/laws/show/2469-19 (accessed: 7.09.2026).

50. On Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII dated October 5, 2017 (as amended). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed: 7.09.2026).

51. On Approval of the Action Plan for 2026 for the Implementation of the Cybersecurity Strategy of Ukraine: Order of the Cabinet of Ministers of Ukraine No. 631-r dated June 24, 2026. URL: https://zakon.rada.gov.ua/laws/show/631-2026-p (accessed: 7.09.2026).

52. European Commission, High Representative of the Union for Foreign Affairs and Security Policy. A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry. JOIN(2024) 10 final. Brussels, 5.3.2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024JC0010 (accessed: 7.09.2026).

53. European Commission. Communication on ProtectEU: a European Internal Security Strategy. COM(2025) 148 final. Strasbourg, 1.4.2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0148 (accessed: 7.09.2026).

54. Partnership and Cooperation Agreement between the European Communities and their Member States, and Ukraine. Official Journal of the European Communities. 1998. L 49. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:1998:049:TOC (accessed: 7.09.2026).

55. Common Strategy of the European Council of 11 December 1999 on Ukraine (1999/877/CFSP). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999E0877 (accessed: 7.09.2026).

56. Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and Ukraine, of the other part. Official Journal of the European Union. 2014. L 161. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2014:161:TOC (accessed: 7.09.2026).

57. Regulation (EU) 2024/792 of the European Parliament and of the Council of 29 February 2024 establishing the Ukraine Facility. URL: https://eur-lex.europa.eu/eli/reg/2024/792/oj (accessed: 7.09.2026).

58. Council Decision (CFSP) 2021/509 of 22 March 2021 establishing a European Peace Facility. URL: https://eur-lex.europa.eu/eli/dec/2021/509/oj (accessed: 7.09.2026).

59. Council Decision (CFSP) 2022/1968 of 17 October 2022 on a European Union Military Assistance Mission in support of Ukraine (EUMAM Ukraine). URL: https://eur-lex.europa.eu/eli/dec/2022/1968/oj (accessed: 7.09.2026).

60. Commission Decision (EU) 2025/1174 of 4 June 2025 recognising certain critical raw material projects located in third countries as Strategic Projects under Regulation (EU) 2024/1252. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025D1174 (accessed: 7.09.2026).

61. On the Decision of the National Security and Defence Council of Ukraine of 14 September 2020 "On the National Security Strategy of Ukraine": Decree of the President of Ukraine No. 392/2020 dated September 14, 2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020 (accessed: 7.09.2026).

62. On the Decision of the National Security and Defence Council of Ukraine of 20 August 2021 "On the Concept for Ensuring the National Resilience System": Decree of the President of Ukraine No. 479/2021 dated September 27, 2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021 (accessed: 7.09.2026).

63. On the Decision of the National Security and Defence Council of Ukraine of 11 August 2021 "On the Economic Security Strategy of Ukraine for the Period until 2025": Decree of the President of Ukraine No. 347/2021 dated August 11, 2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021 (accessed: 7.09.2026).

64. On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine No. 447/2021 dated August 26, 2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (accessed: 7.09.2026).

65. On the Decision of the National Security and Defence Council of Ukraine of 15 October 2021 "On the Information Security Strategy": Decree of the President of Ukraine No. 685/2021 dated December 28, 2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (accessed: 7.09.2026).

66. On Amendments to Certain Laws of Ukraine Concerning Information Protection and Cyber Defence of State Information Resources and Critical Information Infrastructure Facilities: Law of Ukraine No. 4336-IX dated March 27, 2025. URL: https://zakon.rada.gov.ua/laws/show/4336-20 (accessed: 7.09.2026).

67. European Council meeting – Conclusions, 27 June 2024. Joint security commitments between the European Union and Ukraine. URL: https://www.consilium.europa.eu/media/oredhmis/eu-ukraine-security-commitments-en.pdf (accessed: 7.09.2026).

68. European Parliament, Council of the European Union. Regulation (EU) 2025/2643 of 16 December 2025 establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products ('EDIP Regulation'). OJ L, 2025/2643, 29.12.2025. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R2643& (accessed: 7.09.2026).

69. Council of the European Union. Council Implementing Decision (EU) 2026/1354 of 15 June 2026 authorising the provision of support from the EU Cybersecurity Reserve to Ukraine. OJ L, 2026/1354, 16.6.2026. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32026D1354& (accessed: 7.09.2026).

70. ENTSO-E. Continental Europe successful synchronisation with Ukraine and Moldova power systems : press release. 16 March 2022. URL: https://www.entsoe.eu/news/2022/03/16/continental-europe-successful-synchronisation-with-ukraine-and-moldova-power-systems/ (accessed: 7.09.2026).

71. Energy Community Secretariat. Ukraine Energy Support Fund. URL: https://www.energy-community.org/Ukraine/Fund/overview.html (accessed: 7.09.2026).

72. Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. URL: https://eur-lex.europa.eu/eli/dec/2013/1313/oj (accessed: 7.09.2026).

73. Council Decision 2014/512/CFSP of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. URL: https://eur-lex.europa.eu/eli/dec/2014/512/oj (accessed: 7.09.2026).

74. Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. URL: https://eur-lex.europa.eu/eli/reg/2014/833/oj (accessed: 7.09.2026).

75. Council Decision 2014/145/CFSP of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. URL: https://eur-lex.europa.eu/eli/dec/2014/145/oj (accessed: 7.09.2026).

76. Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine. URL: https://eur-lex.europa.eu/eli/reg/2014/269/oj (accessed: 7.09.2026).

77. European Commission. Enhancing the accession process – A credible EU perspective for the Western Balkans. COM(2020) 57 final. Brussels, 5.2.2020. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0057 (accessed: 8.09.2026).

78. Regulation (EU) 2026/1386 of the European Parliament and of the Council of 17 June 2026 on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32026R1386 (accessed: 8.09.2026).

79. Regulation (EU) 2025/2083 of the European Parliament and of the Council of 8 October 2025 amending Regulation (EU) 2023/956 as regards simplifying and strengthening the carbon border adjustment mechanism. URL: https://eur-lex.europa.eu/eli/reg/2025/2083/oj (accessed: 8.09.2026).

CHAPTER 2

ENVIRONMENTAL SECURITY IN UKRAINE IN THE CONTEXT OF THE EUROPEAN GREEN DEAL



2.1. The European Green Deal as a strategic framework for environmental transformation

Environmental safety and energy independence remain key factors in a country's development. For Ukraine, these are particularly relevant in the context of European integration and the implementation of the European Green Deal, which focuses on the rational use of resources and reducing environmental impact. Current models of economic development often led to the inefficient use of natural resources, particularly in the agricultural sector. This hinders their regeneration, depletes biological potential and exacerbates environmental risks; therefore, European integration requires a combination of economic growth and sustainable development. Rational management of agricultural resources involves treating biological capital as a renewable asset, which creates economic advantages during eco-transformation. Integration into the European Green Deal contributes to the modernisation of agricultural production in line with EU standards and to enhancing the competitiveness of Ukrainian products. The potential for environmental change can be assessed using analytical models that compare the state of Ukraine's production and export figures with those of EU countries. The European Green Deal stimulates trade in carbon credits, the development of production and the reduction of greenhouse gas emissions. The environment's assimilation potential ensures the restoration of resources and a reduction in anthropogenic pressure. Ukraine's integration into EU environmental standards requires effective management of the agricultural sector's biological potential to ensure sustainable production and nature conservation [1].

As part of the European Green Deal, the European Union aims to reduce greenhouse gas emissions by 50–55 per cent compared with 1990 levels. This strategy covers key sectors of the economy, including transport, energy, agriculture, construction and industry [2].

As part of the process of aligning with European Union environmental standards, Ukraine's transport policy must place greater emphasis on the modernisation of transport infrastructure and the gradual digitalisation of the sector. This involves updating existing transport networks, improving the efficiency of mobility systems, introducing cleaner and more technologically advanced solutions, and strengthening the institutional capacity needed to manage these changes. Such measures are important because the transport sector has a direct impact on air quality, energy

consumption and the overall level of environmental safety. Therefore, the consistent renewal of infrastructure and the wider use of digital tools can help Ukraine move closer to European Union requirements, improve the coordination of transport policy and strengthen the country's environmental security in the context of European integration.

An analysis of environmental policy at the national's levels makes it possible to assess the effectiveness of the implementation of European environmental protection standards in Ukraine and to improve decision-making in this area. National environmental policy must be comprehensive, as the effectiveness of environmental protection measures and the integration of Ukrainian practices into the European legal framework depend on its coherence. A structural approach makes it possible to assess the impact of the energy sector on environmental performance through the gross domestic product energy intensity indicator. Forecasting this indicator helps to determine the need for stronger regulatory measures. This approach can form the basis for reforming public administration, as energy indicators largely determine the environmental and economic state of related sectors. Applying these approaches enhances the effectiveness of governance, brings Ukraine's environmental policy closer to European Union standards and strengthens the country's environmental security [3].

Clean atmospheric air is one of the essential conditions for maintaining a high quality of life, protecting public health and preserving the stability of natural ecosystems. Air quality directly influences the well-being of the population, the condition of urban environments and the effectiveness of environmental protection measures. In this regard, the experience of the European Union in organising and improving air quality monitoring can be especially useful for Ukraine, as it demonstrates practical approaches to the systematic observation, assessment and management of atmospheric pollution. European monitoring practices combine fixed monitoring stations, which provide continuous and comparable long-term data, with mobile stations that make it possible to respond flexibly to local pollution episodes and assess the situation in different parts of a city. Such an integrated approach ensures the collection of timely, reliable and spatially detailed information, which is necessary for effective environmental management, pollution control and the development of preventive measures. For example, a comparison of air quality in Poltava and Leipzig makes it possible to identify the most effective methods of monitoring and control, evaluate the influence of local urban and meteorological conditions, and use available resources more rationally in order to improve environmental safety [4].

The combination of fixed and mobile monitoring equipment enables Ukrainian cities to bring their air quality control system closer to European standards by ensuring both continuous observation and flexible local assessment. Fixed monitoring stations

provide stable, comparable and long-term data on the concentration of pollutants, while mobile equipment makes it possible to study specific urban areas, identify local pollution episodes and respond more quickly to changes in atmospheric conditions. This approach ensures systematic monitoring of pollution over time, takes into account emerging environmental trends and seasonal fluctuations, and allows responsible authorities to respond promptly to changes in atmospheric air quality. As a result, the integration of both types of monitoring creates a more complete information base for environmental decision-making, supports the planning of preventive measures and improves the overall effectiveness of air quality management in urban areas.

Effective monitoring of air pollution requires the use of digital tools, particularly in conditions where local authorities have limited financial, technical and organisational resources. Such tools make it possible to collect environmental data more systematically, process large volumes of information more quickly and support evidence-based decision-making at the municipal level. In accordance with the European Union's Directive on ambient air quality, modern information systems should not be limited to the simple accumulation of monitoring results; they must integrate data processing, analytical assessment and visual presentation in a unified framework. This combination allows local administrations and environmental services to identify pollution trends, compare indicators over time, interpret spatial differences and communicate the results of monitoring more clearly to decision-makers and the public.

Such systems utilize time-series models, in particular the autoregressive integrated moving average model and exponential smoothing, considering trends and seasonality, whilst automatically selecting the most accurate forecasting approach. Spatial and correlation analyses make it possible to map the distribution of pollutants and establish relationships between them. Using the Kremenchuk conurbation as an example for the period 2007–2024, the system demonstrated its ability to forecast air quality and identify areas where maximum permissible concentrations are exceeded. For certain pollutants, the exponential smoothing model proved to be more accurate. The introduction of such systems provides local authorities with a cost-effective tool for decision-making, optimising monitoring networks and moving closer to European Union standards, thereby enhancing Ukraine's environmental safety [5].

Environmental safety in urbanised areas is a fundamental prerequisite for the sustainable development and long-term resilience of modern cities. In this context, building density, the configuration of urban spaces and the principles of architectural planning play a particularly important role, since they influence the formation of the urban 'heat island' effect. This phenomenon is expressed in higher temperatures within densely built-up city areas compared with surrounding suburban or rural territories and affects not only the thermal regime but also air quality, energy consumption, public

comfort and overall environmental conditions. The intensity of the heat island effect depends on a combination of factors, including local climatic characteristics, the density and height of buildings, the availability and distribution of green spaces, the presence of water bodies, the type of road surfaces, traffic volume and the operation of heat-generating facilities. Therefore, a comparison of temperature indicators in urban and adjacent rural areas makes it possible to assess the scale of urbanisation's impact on the local climate and to identify the main sources of thermal anomalies. For a more comprehensive analysis, it is necessary to consider the spatial location of parks, tree plantations, reservoirs, transport infrastructure and artificial surfaces that accumulate and retain heat. Combining these data with modern meteorological measurements, digital monitoring tools and spatial analysis methods allows researchers to determine the structure and dynamics of thermal anomalies within the urban environment. The identified patterns confirm the need for further study of the interaction between anthropogenic sources, transport flows, water bodies and green infrastructure in shaping the city's microclimate. Such research provides a scientific basis for developing effective environmental strategies, improving urban planning decisions, reducing heat stress and enhancing the quality of life in urbanised areas. The obtained results should be taken into account in strategic planning and public policy, since the combination of scientific analysis, digital monitoring and public participation strengthens air quality control, supports sustainable urban development and helps build trust between authorities and citizens [6].

The application of such approaches enhances the level of environmental safety in Ukraine's urbanised areas and helps to align national monitoring practices with the experience of the European Union, where public participation in monitoring the state of the environment is a key element of sustainable development policy and of improving the quality of life for the population. Over recent decades, public and business interest in environmental issues has grown significantly due to the increasing negative impact of human activity on the environment. Population growth and density, industrial development and the rise in transport volumes are causing the degradation of natural ecosystems. The constant increase in environmental damage necessitates effective financial mechanisms capable of ensuring the timely and full compensation of harm caused by environmental incidents to individuals and legal entities, as well as the restoration of the environment to the regulatory standards required for people to live safely [7].

Environmental insurance is an effective tool for addressing these challenges; it is widely used in European Union member states and is gradually gaining ground in Ukraine. Its role is to ensure that businesses are financially liable for damage caused to the environment, to encourage environmentally sound practices, and to enhance preparedness for climate and environmental risks. Climate change is a complex process

within the Earth system, characterised by threshold states and non-linear dynamics. In this context, environmental insurance should ensure a response to climate threats and maintain financial stability in the event of environmental incidents. Experience in Ukraine and the European Union shows that mitigating the consequences of such risks is important both for the insurance sector and for society, although even developed insurance systems often remain predominantly adaptive. The approach of comprehensive adaptive systems makes it possible to assess the long-term effectiveness of insurance mechanisms and to shape the direction of their further development for the sustainable management of climate risks. Its application contributes to the modernisation of environmental insurance, the improvement of financial coverage for environmental losses, and the strengthening of society's capacity to respond to the consequences of climate change. This is important for the development of reliable insurance systems in Ukraine and for bringing them into line with European standards for environmental risk management [8].

Ukraine's transition to a green economy is a key component of its strategy for sustainable development and European integration. It involves combining economic performance, social responsibility and environmental sustainability through the rational use of resources, the development of renewable energy and the reduction of negative environmental impacts. Of particular importance is an analysis of the conditions for the development of the agricultural sector, its qualitative changes and strategic planning, considering European integration, military challenges and the needs of post-war reconstruction [9].

An assessment of Ukraine's environmental legislation and the scientific approach to evaluating its effectiveness highlights the need for coordinated sectoral reforms. Priorities include biodiversity conservation, industrial pollution prevention, modern waste management, stricter emissions control, reliable environmental monitoring and stronger liability for environmental harm. As these areas are interconnected, progress requires consistent regulatory, institutional and financial support. In post-war reconstruction, environmental policy should be regarded as an essential condition for territorial recovery, public health protection and ecosystem resilience. Effective implementation also depends on regulatory compliance, transparent enforcement and improved mechanisms for assessing and compensating environmental damage. Green innovation, environmental auditing and certification, cooperation among public authorities, businesses and research institutions, and greater support for environmental research would strengthen evidence-based policy and facilitate alignment with European standards. Together, these measures can establish integrated environmental governance and ensure that Ukraine's reconstruction supports long-term sustainable development [10].

An important area of further development is the deepening of Ukraine's integration with the European Union in resource conservation and energy efficiency. This process supports the alignment of national approaches with European standards, improves energy efficiency in key sectors, strengthens waste management and creates favourable conditions for environmentally oriented innovation. Its implementation requires the modernisation of industrial facilities, housing and communal infrastructure, transport systems and energy networks, together with technologies that reduce energy and material consumption. Attention should be paid to renewable energy, circular economy principles, material reuse and recycling, and improved monitoring of resource consumption. Cooperation with the European Union also provides access to expertise, financial instruments and research programs that can accelerate green projects and strengthen institutional capacity. European integration in these areas is a strategic foundation for a resilient, resource-efficient and competitive model of Ukraine's sustainable development.

2.2. Harmonisation of Ukraine's environmental policy and EU legislation

The alignment of Ukraine's environmental legislation with European Union law covers key areas of environmental protection, in particular the regulation of water resources and waste management. At the same time, the national regulatory framework already partially complies with the obligations set out in the Association Agreement between Ukraine and the European Union. However, difficulties remain in the practical implementation of the adopted regulations, strategies and action plans. The most pressing issues remain the adaptation of water legislation to European requirements and the improvement of the solid municipal waste management system. To assess the progress of reforms and identify further priorities for harmonising Ukrainian legislation with European Union standards, it is advisable to apply comparative legal, statistical, analytical and logical approaches. The introduction of European practices contributes to improving the effectiveness of environmental management in Ukraine, integrating national approaches into the European framework and strengthening the country's environmental security.

Legislative changes have strengthened citizens' involvement in environmental impact assessment by requiring enterprises, before making final decisions, to evaluate how their activities may affect water bodies, air quality and natural sites, while also

ensuring meaningful public participation and due consideration of every submitted opinion [11].

At both the international level and within the European Union, a broad and systematic set of legal mechanisms has been developed to address climate change, adapt to its consequences and reduce related environmental risks. These mechanisms include legal norms, regulatory instruments and policy frameworks that are aimed at limiting the negative effects of climate processes on ecosystems, economic activity and public well-being. The European Union plays a particularly important role in this area, as it actively shapes legislation designed to reduce greenhouse gas emissions, primarily through the operation of the emissions trading scheme. In addition, European regulation covers the use of fluorinated gases and ozone-depleting substances, which are recognised as significant factors influencing climate stability and atmospheric protection. As an associated state of the European Union, Ukraine is gradually introducing these environmental standards into its national legal and institutional system. Under the Association Agreement, this process involves the approximation of Ukrainian legislation to European Union requirements, the establishment of mechanisms for controlling greenhouse gas emissions, the regulation of hazardous substances and the promotion of sustainable use of natural resources. Such implementation strengthens Ukraine's environmental policy and supports its broader integration into the European legal and environmental framework.

The development of international and European legal instruments in the field of climate policy demonstrates the growing responsibility of states for environmental protection and the achievement of sustainable development. The effectiveness of these measures depends on coordinated action by countries and public support for the implementation of environmental standards. The key principles of the Green Deal define the transition to a sustainable and environmentally balanced economy. The first principle involves recognising natural capital as a key driver of economic development and integrating it into models of economic growth. This principle entails taking environmental externalities into account, improving resource and energy efficiency, and creating decent and sustainable jobs. The second principle aims to conserve biodiversity and ecosystems through investment in natural capital and its restoration. It emphasises the need to respect planetary boundaries and environmental constraints, as well as to support the achievement of international environmental sustainability goals. The third principle focuses on ensuring social justice and the well-being of the population. Its implementation involves reducing poverty, expanding access to basic services and social protection systems, developing inclusive and democratic governance, and upholding the principles of equality and justice between countries, social groups and generations. These principles form the basis for sustainable development, the conservation of natural resources and the protection of the

environment for future generations. Their implementation requires cooperation between governments, business and the public at both national and international levels [12].

The strategic objectives of the Green Deal define the main directions for the transition to sustainable development and for the systematic reduction of negative environmental impacts. They provide a framework for transforming key sectors of the economy in a way that links environmental protection with technological renewal, economic modernisation and social responsibility. One of the central priorities is the introduction of clean technologies and the comprehensive modernisation of infrastructure. This objective involves replacing outdated, resource-intensive and environmentally harmful solutions with safer and more sustainable alternatives in manufacturing, transport, construction and other important sectors. Such changes are intended not only to reduce pollution, but also to improve production efficiency, encourage technological innovation and create conditions for long-term environmental resilience. Another key objective is to improve energy efficiency across all areas of public life, including industry, transport, construction, public services and households. More efficient use of energy allows societies to reduce overall resource consumption, decrease dependence on carbon-intensive energy sources and limit greenhouse gas emissions. It also contributes to lower operating costs, more rational use of infrastructure and a gradual reduction in the negative effects of human activity on the climate. In this sense, energy efficiency is not only a technical requirement, but also an important element of sustainable economic transformation and environmental security. A further strategic objective is to support innovation and attract investment in green projects. To achieve this, it is necessary to create favourable institutional and economic conditions for the development of environmentally friendly technologies through financial incentives, tax benefits, public support for research and targeted program for environmental initiatives. Investment in green projects can accelerate the introduction of new solutions, strengthen the competitiveness of sustainable industries and encourage cooperation between the state, business, research institutions and civil society. Overall, these objectives are aimed at building a sustainable, competitive and environmentally balanced society. Their achievement requires coordinated action by the state, business and the public, as well as the development of international cooperation aimed at conserving natural resources and protecting the environment. The implementation of these priorities therefore forms an important basis for a long-term green transition, in which economic development is combined with environmental responsibility and the preservation of favourable living conditions for present and future generations.

The Green Deal is aimed not only at protecting the environment, but also at achieving significant and long-term economic results. Its implementation stimulates

the emergence and expansion of new markets in the fields of renewable energy, energy efficiency and green technologies, thereby creating additional opportunities for business development, investment activity and employment growth. By encouraging the use of environmentally oriented innovations, the green transition can support the modernisation of production processes, increase the competitiveness of enterprises and promote the development of sectors that are less dependent on carbon-intensive resources. Another important economic benefit is the gradual reduction of dependence on expensive and volatile energy resources. The wider use of renewable energy sources decreases the need to import oil and gas, strengthens national energy security and reduces the vulnerability of economies to price fluctuations on global energy markets. Reducing pollution also makes it possible to lower public and private expenditure on environmental protection measures and healthcare. Lower emissions reduce the need for costly remediation of air, water and soil and, at the same time, decrease the risks of diseases associated with environmental degradation. Consequently, the economic advantages of the green transition combine the stimulation of economic development, the reduction of environmental pressure and the formation of a more sustainable and resilient society. Achieving these results requires consistent policy support, long-term investment and coordinated cooperation between the state, business and the public.

Thus, the Green Deal can help Member States fully realise the economic and employment benefits of the green transition by generating new environmentally oriented jobs, supporting stable and sustainable growth, reducing pollution and improving air quality for healthier living conditions [13].

The social benefits of the Green Deal are reflected in an improved quality of life and better public health. One of the key outcomes is an improvement in air and water quality thanks to a reduction in emissions of harmful substances and pollutants. Cleaner air reduces the risks of respiratory diseases, allergies and other health problems linked to air pollution. Another important social benefit is the reduction in the negative impact of pollution on people's health. [14] Lower levels of environmental pollution, reduced greenhouse gas emissions and improved water quality help to reduce the prevalence of respiratory, allergies, skin and other diseases. Consequently, the green transition has a positive impact on the health and well-being of society, as reducing pollution and improving the state of the environment help to enhance the quality of life. Its implementation combines environmental protection with care for citizens' health, making this approach a key factor in sustainable development.

The political challenges of green development require a systematic approach and enhanced international cooperation [15]. As environmental problems are global in nature, cooperation between states is essential to reduce greenhouse gas emissions, conserve biodiversity and ensure the sustainable use of natural resources. Another key area is the introduction of effective regulatory mechanisms to ensure that

environmental commitments are met. To this end, governments must take strategic decisions and establish legal frameworks, tax incentives and financial instruments that steer businesses towards reducing their environmental impact. Such mechanisms may include setting mandatory targets for the use of renewable energy, developing an emissions trading scheme and supporting green projects. They not only monitor compliance with commitments but also encourage environmental initiatives.

Therefore, the transition to sustainable and environmentally sound development requires the active participation of all stakeholders, including governments, businesses, civil society institutions and local communities, as well as coordinated action at the international level. Such cooperation is necessary because environmental challenges extend beyond national borders and require common principles, shared responsibility and consistent policy implementation. Policy strategies must therefore be oriented towards shaping an environmentally balanced future by combining regulatory measures, economic incentives, public engagement and long-term planning. In this way, political decisions can support the gradual transformation of economic and social systems while preserving natural resources, reducing environmental risks and strengthening the foundations of sustainable development.

2.3. Environmental threats and challenges in Ukraine in the context of the war

An analysis of publications by Ukrainian and international researchers shows that the full-scale war has become an unprecedented factor in the degradation of Ukraine's environment, the consequences of which affect all key natural components: atmospheric air, water resources, soil, biodiversity and nature conservation areas. Scientists unanimously note that hostilities not only cause local environmental disturbances in areas of direct conflict but also pose long-term risks to the country's environmental security as a whole. War inflicts irreparable damage on air quality, water bodies, soil cover, flora and fauna, as well as public health, and the scale of the destruction allows it to be viewed through the lens of ecocide. The environmental consequences of war are viewed as the result of deliberate actions leading to large-scale damage to natural ecosystems, pollution of the atmosphere, water resources and soil, the destruction of biodiversity and the disruption of the ecological balance. Emphasis is placed on the fact that the scale of the damage inflicted raises the issue of the recognition of such actions as ecocide under international law and the need to establish effective mechanisms for holding the perpetrators to account [16].

In the study [17], the environmental consequences of war are examined in the context of ecological and economic security. The researchers emphasise that military aggression has led to the pollution of air, water and soil, as well as the destruction of landscapes, natural ecosystems and high-risk infrastructure facilities, in particular nuclear, hydro-engineering, chemical and metallurgical plants. Considerable attention is paid to the threats to nature reserves and the marine ecosystems of the Black and Azov Seas. The destruction of industrial enterprises, energy facilities, transport infrastructure and natural complexes creates a range of risks that extend far beyond the sphere of environmental protection. Environmental pollution, damage to water resources, land degradation and the threat of man-made accidents directly affect the state's defence capability, the economic stability of regions and the safety of the population. The issue of damage assessment is considered in the context of ensuring ecological and economic security. Scholars note that the destruction of natural resources and the pollution of land, water bodies and the atmosphere result in significant economic losses that require comprehensive accounting. They emphasise the need for interdisciplinary approaches that combine environmental, economic and security criteria for assessing the consequences of war.

The complexity of the assessment stems from the long-term nature of many of the war's consequences, which may persist for a considerable time after the end of hostilities. In this regard, continuous monitoring of the state of the environment, the collection of reliable data and the development of standardised methodologies for determining losses are of particular importance. Environmental damage is examined through the lens of atmospheric air pollution resulting from shelling of industrial facilities and oil depots, soil degradation caused by explosions, fires and landmines, loss of biodiversity and depletion of water resources. Scientists also highlight the destruction of the Kakhovka Hydroelectric Power Station as one of the most significant manifestations of the environmental disaster, which has led to the disruption of aquatic ecosystems, the flooding of territories, the loss of flora and fauna, and the deterioration of the water supply. The destruction of industrial enterprises, energy and water management infrastructure, the pollution of land and water resources, and the destruction of natural ecosystems bear the hallmarks of actions whose consequences extend beyond local environmental disturbances. Particular attention is paid to the need to document such facts, build up a body of evidence and develop procedures for an international legal response to the environmental consequences of the war [18].

The main causes of environmental degradation include explosions of munitions, the use of heavy machinery, fires, military waste, the mining of land and the destruction of natural habitats. The consequences include air pollution from toxic substances and greenhouse gases, the entry of pollutants into surface and groundwater, soil degradation, the forced migration of animals, a decline in species populations and the

deterioration of protected areas. Particular emphasis is placed on the link between environmental losses and risks to public health, including respiratory diseases, deterioration in drinking water quality and food insecurity [19].

The relevance of these issues is confirmed by research into geo-ecological threats, the deepening biodiversity crisis, the consequences of land mining, damage to forest ecosystems and other manifestations of the impact of war on the natural environment. Scientific research emphasises the use of geoinformation technologies, spatial analysis, remote sensing and field studies to identify environmental changes, assess the state of ecosystems and determine the extent of anthropogenic impact. In the context of military operations, such tools take on particular significance for monitoring damaged territories and natural complexes [20]. Environmental security is regarded as an integral element of a state's national security system, directly affecting economic stability, the protection of the population, the functioning of critical infrastructure and the state's ability to counter internal and external threats. Scholars are moving away from the traditional understanding of environmental security as a purely nature conservation category and interpret it as a comprehensive security factor that determines the conditions for a country's sustainable development during wartime and post-war reconstruction.

Scientists emphasise that the degradation of the natural environment, the depletion of natural resources and the rise in man-made risks pose direct threats to people's livelihoods and require a systematic legal and institutional response. Attention is paid to improving the mechanisms of state environmental policy and safeguarding citizens' environmental rights. The researchers emphasise the importance of properly documenting environmental offences, improving state control mechanisms and developing a regulatory framework that would ensure the effective assessment of the extent of environmental damage and liability for causing it. An important task is identified as the formation of a comprehensive environmental management system capable of ensuring proper accounting for and compensation of damages. The adaptation of legislation is regarded as an important condition for strengthening environmental security and establishing a modern system of environmental regulation [21].

Environmental security is analysed through the prism of the state's economic and food security. It is emphasised that the deterioration of natural resources and environmental pollution have a negative impact on productive capacity, the investment attractiveness of regions, the agricultural sector and the ability to ensure food security. Consequently, environmental risks are viewed as factors capable of transforming into large-scale socio-economic threats. An adequate evidence base is a prerequisite for subsequently holding those responsible to account and implementing compensation

mechanisms. Of particular importance is the harmonisation of approaches to determining environmental damage in accordance with international standards [22].

Scholars note that ensuring a sound environment is a fundamental condition for maintaining public health, social stability and the regeneration of natural resource potential. Environmental security is regarded as one of the key areas of state policy on sustainable development and an element in ensuring citizens' quality of life [23].

The issue of sustainable development is examined through the interconnection of economic, social and environmental processes, which have undergone significant transformations under the influence of Russian military aggression. Scholars emphasise that the war has created a systemic crisis which has simultaneously affected the state's productive capacity, the social sphere and the natural environment, calling into question the feasibility of traditional models of sustainable development. In this context, the search for new approaches to post-war reconstruction – which would take into account not only economic growth but also environmental security and social resilience – has become particularly relevant.

The war has brought about profound structural changes in the economy, exacerbated regional disparities, and worsened the investment climate, whilst at the same time highlighting the need to implement development models focused on resource efficiency, innovation and long-term sustainability. Attention is paid to the role of public policy in restoring economic activity and ensuring balanced regional development. Post-war reconstruction must be based on innovative development, resource efficiency and the introduction of new technologies capable of ensuring long-term economic sustainability. Recovery is viewed as an opportunity to modernise the manufacturing sector and lay the foundations for a more balanced national development [24]. Widespread damage to natural resources, environmental pollution, the destruction of ecosystems and the deterioration of living conditions for the population pose significant constraints on the country's post-war recovery. War is seen as a factor that exacerbates environmental risks and intensifies the conflict between the economic needs of reconstruction and the necessity of preserving natural capital. At the same time, it is emphasised that Ukraine's recovery must be based on the principles of greening economic activity, the rational use of natural resources and compliance with international environmental safety standards. The process of European integration is linked to the need to make Ukraine's post-war development more environmentally sustainable. European approaches are regarded as a benchmark for shaping long-term environmental security policy and minimising the impact of war on the environment [25].

Considerable attention is paid to analysing the large-scale destruction of the natural environment resulting from Russian military aggression through the prism of ecocide and war crimes against the environment. Scholars emphasise that the

environmental consequences of the war go beyond ordinary pollution or the degradation of natural resources, as they are systemic in nature, cover vast territories and pose long-term risks to ecosystems, the economy and public health.

The scale of the environmental damage caused by the war requires not only its documentation but also the creation of a scientifically sound system for assessing losses, which could be used to legally protect the state's interests, secure compensation for losses and plan the restoration of affected territories. Ukraine's post-war recovery is viewed not merely as a process of rebuilding destroyed infrastructure and the economy, but as an opportunity to carry out a profound environmental modernisation of the state based on the principles of sustainable development. Academics emphasise that the consequences of the war necessitate the development of a new model of development that will combine economic recovery with environmental security, the rational use of natural resources and the implementation of modern environmental protection standards.

Green recovery is linked to the transition to an environmentally oriented economic model. Significant attention is being paid to the development of renewable energy, improving energy efficiency, reducing the resource intensity of production, and introducing low-carbon technologies. Academics emphasise that post-war reconstruction must take into account contemporary climate challenges and align with the objectives of the economy's green transition [26].

The path towards European integration is regarded as a key prerequisite for the structural modernisation of the economy. Scholars emphasise that alignment with European approaches contributes to enhancing the competitiveness of the national economy, developing innovative sectors and implementing the principles of resource efficiency. In this context, integration with the EU is seen as a mechanism for shaping a new model of economic growth, focused on long-term sustainability and balanced development. The implementation of European environmental standards involves the adoption of principles of climate responsibility, the development of energy-efficient technologies, the reduction of the negative impact of economic activity on the environment, and the expanded use of environmental management tools. At the same time, adaptation to EU requirements is seen as a key factor in enhancing the country's investment attractiveness and ensuring its long-term socio-economic sustainability [27].

Environmental monitoring is regarded as one of the key tools for ensuring environmental safety during wartime and post-war reconstruction. Scientists emphasise that the scale of war damage and the significant spatial and temporal variability of environmental processes require the use of modern technologies for observation, data collection and analysis. It is precisely high-quality monitoring that is identified as a necessary prerequisite for recording environmental damage, assessing

risks, making management decisions and planning nature conservation measures [28]. The use of modern digital technologies is regarded as the basis for improving the effectiveness of environmental monitoring. The importance of remote sensing, geoinformation systems, satellite data and integrated information platforms for assessing the state of natural resources is emphasised. Such approaches make it possible to obtain up-to-date information on changes in the environment, analyse the spatial distribution of adverse processes and forecast the future development of the environmental situation.

2.4. Ukraine's green post-war recovery: implementing European climate and ecological standards

The transition to a green economy requires a comprehensive approach and the resolution of a wide range of problems and challenges. It is important for governments, businesses and the public to play an active role in developing and implementing effective strategies that will promote sustainable and environmentally balanced development.

What steps should Ukraine take to prevent climate change and adapt to its consequences?

– Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC [29].

– Regulation (EC) No 2037/2000 of the European Parliament and of the Council of 29 June 2000 on substances that deplete the ozone layer [30].

– Regulation (EC) No 842/2006 of the European Parliament and of the Council of 17 May 2006 on certain fluorinated greenhouse gases [31].

Directive 2003/87/EC is one of the European Union's key legislative acts in the field of reducing greenhouse gas emissions and combating global warming. The document sets out the principles and instruments governing the operation of the Community-wide emissions trading scheme, which aims to reduce emissions and mitigate the overall anthropogenic impact on the climate system.

One of the key provisions of the Directive is the introduction of emission caps and allowances for greenhouse gases in specific industrial and energy sectors. This regulatory approach incentivises economic operators to reduce emissions, improve the efficiency of production processes and adopt technologies with a lower environmental impact. At the same time, the Directive creates the conditions for the development of

innovative technologies and methods to reduce greenhouse gas emissions. The introduction of a market-based emissions trading mechanism creates an economic incentive to develop and apply modern solutions that enable emissions to be reduced and the environmental performance of economic activities to be improved.

Furthermore, the provisions of the Directive support the development of a market for green technologies within the Community. The operation of the emissions trading scheme creates a favourable economic environment for the development, implementation and commercialisation of environmentally sound solutions, thereby expanding new market segments and stimulating the growth of environmentally oriented industries.

Consequently, Directive 2003/87/EC is a significant instrument for steering the European Union towards a model of sustainable development and limiting human-induced climate change. The implementation of its provisions contributes to achieving energy efficiency targets and reducing greenhouse gas emissions, and consequently to improving the state of the environment and ensuring the long-term sustainable development of the Community.

European Union Regulation 2037/2000 is a significant regulatory instrument aimed at protecting the ozone layer and minimising threats to the environment and public health. Its provisions prohibit the production and use of substances capable of depleting the ozone layer, in particular chlorofluorocarbons (CFCs), halons, brominated fluorocarbons and other ozone-depleting compounds.

The key principles of Regulation 2037/2000 provide for the introduction of mechanisms to monitor the circulation of hazardous substances, as well as the gradual phase-out of their production and use. The implementation of these requirements ensures the phased decommissioning of equipment and processes that use such compounds and helps to reduce their damaging impact on the ozone layer. Regulation also encourages the adoption of safer alternative substances and technologies that do not deplete the ozone layer. The transition to such solutions enhances environmental protection and reduces the risks to public health associated with the adverse effects of ozone-depleting compounds.

Consequently, Regulation 2037/2000 is a key component of international measures to protect the ozone layer and achieve sustainable development goals. Proper implementation and compliance with its provisions contribute to the creation of environmentally safe living conditions and the preservation of a favorable environment for future generations.

European Union Regulation 842/2006 is one of the leading regulatory mechanisms for combating climate change and laying the foundations for sustainable development. Its provisions set out restrictions and requirements regarding the production and use of certain fluorinated greenhouse gases, which are characterised by a high global warming potential and have a significant impact on the climate system.

One of the key objectives of Regulation 842/2006 is to reduce the release of fluorinated greenhouse gases into the atmosphere and to strengthen controls on their recovery. To achieve this objective, the Regulation sets out measures aimed at introducing effective technological solutions and encouraging the use of alternative substances that do not have a harmful impact on the climate.

The Regulation also promotes the introduction of innovative technologies aimed at reducing the use of fluorinated greenhouse gases. These include the development of new production methods, the use of alternative materials and the improvement of energy-saving technologies.

An important aspect of the Regulation is the promotion of green alternatives and environmentally sound solutions in the use of fluorinated greenhouse gases. This involves supporting scientific research and innovation in the relevant sector, as well as providing financial incentives and benefits to businesses that adopt environmentally friendly technologies.

Overall, Regulation 842/2006 is a key component of global efforts to combat climate change and build a sustainable future. The implementation of its provisions helps to mitigate the negative impact on the climate system and contributes to the preservation of the health and proper functioning of ecosystems.

In 2016, the Cabinet of Ministers of Ukraine took an important step in tackling climate change by approving the Concept for the Implementation of State Policy on Climate Change for the period up to 2030. This document sets out the strategic framework for the state's activities aimed at mitigating the effects of global warming and adapting to climate change. The Concept covers a range of interrelated areas, including energy, industry and transport, as well as the socio-economic and environmental components of state policy.

In 2017, with a view to putting the provisions of the Concept into practice, a corresponding action plan was approved, setting out specific areas of activity and tasks for achieving the defined objectives. The document provided for a wide range of measures, including the development of renewable energy, the reduction of greenhouse gas emissions and the improvement of energy efficiency.

In 2018, Ukraine set out long-term climate policy objectives by adopting the Low-Carbon Development Strategy up to 2050. The document sets out the state's vision of a consistent transition to a low-carbon development model. The strategy establishes specific goals, objectives and instruments necessary to reduce greenhouse gas emissions and improve energy efficiency.

These decisions demonstrate the consistency of Ukraine's commitments in the field of environmental protection and combating climate change. They confirm that ensuring sustainable development and protecting the natural environment are defined as priority areas of national policy.

The expected consequences of implementing European Union (EU) legislation in the field of environmental protection and combating climate change are of crucial importance for countries committed to building a sustainable and environmentally balanced future. First and foremost, the implementation of the relevant legal provisions will contribute to a significant reduction in greenhouse gas emissions and other atmospheric pollutants, which will improve the state of the environment and have a positive impact on public health.

Furthermore, it is anticipated that the alignment with EU legislation will stimulate the development of cutting-edge technologies and innovative solutions in the fields of renewable energy and environmental protection. This will create additional conditions for the expansion of green markets and increased employment, particularly in the sectors of renewable energy, energy efficiency and environmental innovation.

The implementation of EU standards should also ensure increased energy efficiency across all areas of public life. As a result, energy consumption will be reduced, the competitiveness of the states will be strengthened and consumers' energy costs will fall, which is an important prerequisite for sustainable economic development. At the same time, the implementation of EU legislation will promote the wider use of renewable energy sources and a gradual reduction in dependence on coal and petroleum products. This will enable Member States to reduce their external energy dependence, strengthen energy security and ensure more sustainable development of the energy sector.

Overall, the implementation of EU legislation in the field of environmental protection and combating climate change will bring about significant positive outcomes, promote sustainable development, reduce pollution levels and improve the quality of the natural environment for future generations.

One of the defining early events in the shaping of EU environmental policy was the election on 16 July 2019 by the European Parliament of Ursula von der Leyen, the former German Defence Minister, as President of the European Commission. This decision was of historic significance, as she became the first woman to head the European Commission. Her five-year term began on 1 November 2019. Ursula von der Leyen outlined a number of priority environmental initiatives aimed at strengthening the EU's environmental policy and combating climate change. These include the transformation of part of the European Investment Bank into the European Climate Bank, designed to mobilise one trillion euros in investment for sustainable financing. Another key initiative was the adoption of the Biodiversity Strategy to 2030, aimed at halting the loss of natural resources over the next five years.

The new Circular Economy Action Plan, which applies in particular to the textile and construction sectors, is also one of Ursula von der Leyen's strategic environmental initiatives. The pursuit of the ambitious "zero pollution" target and support for the "farm-

to-fork" strategy demonstrates the intensive roll-out of the EU's environmental policy under her leadership. The proposed measures have significant potential to improve the state of the environment and enhance the health of the European Union's population.

In August 2019, the European Commission presented "Horizon Europe" as the EU's future investment program for research and innovation for the period 2021–2027. It was intended to succeed the previous 'Horizon 2020' initiative. The presentation materials outlined the program's structure and identified its main priority areas. According to the proposed concept, the structure of 'Horizon Europe' comprises three core components: science, innovation and global challenges, aimed at strengthening the competitiveness of European industry. The program also provides for a system of clusters, whose activities are aimed at tackling global challenges and achieving sustainable development goals. One of the environmentally focused areas is Cluster 5, which brings together issues relating to climate, energy and mobility. Its main purpose is to develop innovative approaches to combating climate change, as well as to promote the development of sustainable energy and environmentally balanced transport systems. Another area is represented by Cluster 6, which covers food, the bioeconomy, natural resources, agriculture and the environment. Its main objectives include strengthening food security, ensuring the rational use of natural resources and preserving the natural environment. The proposed architecture of the 'Horizon Europe' program demonstrates the significant role of environmental issues in the European Union's overall development strategy and reaffirms its commitment to supporting sustainable development, the rational use and conservation of natural resources.

The European Green Deal therefore plays a significant role in the European Union's (EU) sustainable development strategy for the environmental sector and, if properly implemented, has considerable potential to strengthen the economy and ensure long-term sustainability. It encompasses a system of interlinked measures aimed at reducing the human impact on the environment and improving the quality of life for the population. One of the key objectives of this agenda is the transition to environmentally sound technologies and the wider use of renewable energy sources. Implementation of this approach will help to reduce environmental pollution and dependence on coal and petroleum products, whilst also creating further opportunities for the expansion of green markets and the creation of jobs in the renewable energy and green technology sectors. Furthermore, the European Green Deal envisages improving energy efficiency across all areas of public life, which will help to reduce energy consumption and ensure a more rational use of resources. Another key component of this policy is the promotion of innovation and the attraction of investment in green projects, as this accelerates the development of modern technologies and the widespread adoption of environmentally sound solutions across various sectors of the economy. The successful implementation of the European Green Deal has the potential to ensure a balance between economic

prosperity, environmental sustainability and social justice. Its implementation creates new opportunities for the emergence of innovative industries and contributes to the development of a balanced economic model focused on the prudent use and conservation of natural resources for future generations.

References

1. Labenko, O., Sobchenko, T., Hutsol, T., Cupiał, M., Mudryk, K., Kocira, A., ... & Neuberger, P. (2022). Project environment and outlook within the scope of technologically integrated European green deal in EU and Ukraine. *Sustainability*, *14*(14), 8759 https://doi.org/10.3390/su14148759

2. Von Homeyer, I., Oberthur, S., & Dupont, C. (2022). Implementing the European Green Deal during the evolving energy crisis. *J. Common Mkt. Stud.*, *60*, 125. https://doi.org/10.1111/jcms.13397

3. García-Álvarez, M. T., & Moreno, B. (2018). Environmental performance assessment in the EU: A challenge for the sustainability. *Journal of cleaner production*, *205*, 266-280. https://doi.org/10.1016/j.jclepro.2018.08.284

4. Maksiuta, N., Golik, Y. (2020). Comparative Analysis of Pollution of Atmospheric Air in Cities (an Example of Leipzig and Poltava). In: Blikharskyy, Z., Koszelnik, P., Mesaros, P. (eds) Proceedings of CEE 2019. CEE 2019. *Lecture Notes in Civil Engineering*, vol 47. Springer, Cham. https://doi.org/10.1007/978-3-030-27011-7_33

5. Vadurin, K., Perekrest, A., Bakharev, V., Shendryk, V., Parfenenko, Y., & Shendryk, S. (2025). Towards Digitalization for Air Pollution Detection: Forecasting Information System of the Environmental Monitoring. *Sustainability*, *17*(9), 3760. https://doi.org/10.3390/su17093760

6. Golik Yu., Illiash O., Maksiuta N. Urban "Heat-Island Effect" and its Connection with Architectural and Climatic Features on the Example of Poltava. *International Journal of Engineering & Technology*. 2018. Vol. 7, No. 3.2. P. 597–601. https://doi.org/10.14419/ijet.v7i3.2.14598

7. Saif-Alyousfi, A. Y. H., & Alshammari, T. R. (2025). Environmental Sustainability and Climate Change: An Emerging Concern in Banking Sectors. *Sustainability*, *17*(3), 1040. https://doi.org/10.3390/su17031040

8. Demianchuk, M., and Bezpartochna, O. (2023). Development of risk types of insurance in Ukraine under conditions of uncertainty in the context of European integration. Current issues of the management of socio-economic systems in terms of globalization challenges, 151–198. https://doi.org/10.5281/zenodo.7798094.

9. Kovalenko, A., Tsybulska, J., Sakal, O., Krupin, V., & Bratinova, M. (2025). Ukraine's agricultural and rural development : transformation of strategic planning within the processes of European integration. European Research Studies Journal, 28(1), 739-760.

10. Dovgal, O., & Goncharenko, N. (2026). Green recovery and sustainable development in OECD states and Ukraine: Comparative assessment, policy adaptation, and environmental reconstruction in a post-crisis context. *Bank and Policy*, *6*(1), 7-25. https://doi.org/10.56334/bpj/6.1.1

11. Klymenko, V. (2024). Public administration of environmental safety in Ukraine and EU countries. *Law. Human. Environment*, *4*(15), 9-30. https://doi.org/10.31548/law/4.2024.09

12. Adamowicz, M. (2022). Green deal, green growth and green economy as a means of support for attaining the sustainable development goals. *Sustainability*, *14*(10), 5901. https://doi.org/10.3390/su14105901

13. García Vaquero, M., Sánchez-Bayón, A., & Lominchar, J. (2021). European green deal and recovery plan: green jobs, skills and wellbeing economics in Spain. *Energies*, *14*(14), 4145. https://doi.org/10.3390/en14144145

14. Haines, A., & Scheelbeek, P. (2020). European Green Deal: a major opportunity for health improvement. The Lancet, 395(10233), 1327-1329. https://doi.org/10.1016/S0140-6736(20)30109-4

15. Adanma, U. M., & Ogunbiyi, E. O. (2024). A comparative review of global environmental policies for promoting sustainable development and economic growth. *International Journal of Applied Research in Social Sciences*, *6*(5), 954-977. https://doi.org/10.51594/ijarss.v6i5.1147

16. Madzhd, S. M. (2023). Environmental challenges to sustainable development of society under conditions of military actions. *Institutional Repository of National University of Food Technologies*.

17. Onyshchenko, S. V., Masliy, O. A., & Buriak, A. A. (2023). Threats and risks of ecological and economic security of Ukraine in the conditions of war. In 17th *International Conference Monitoring of Geological Processes and Ecological Condition of the Environment* (Vol. 2023, pp. 1-5). European Association of Geoscientists & Engineers. https://doi.org/10.3997/2214-4609.2023520072

18. Polukarov, Y., Kachynska, N., Polukarov, O., Zemlyanska, O., & Mitiuk, L. (2024). Impact of the full-scale war in Ukraine on the environment: *Environmental damage assessment. Law Human Environment*, 15(1), 85–100. https://doi.org/10.31548/law/1.2024.85

19. Filho, W. L., Eustachio, J. H. P. P., Fedoruk, M., & Lisovska, T. (2024). War in Ukraine: an overview of environmental impacts and consequences for human health. *Frontiers in Sustainable Resource Management*, 3. https://doi.org/10.3389/fsrma.2024.1423444

20. Murashchuk, A. I., & Korol, K. A. (2024). Ekolohichni zahrozy ta vyklyky vidbudovy [Environmental threats and challenges of reconstruction]. In *Proceedings of the 5th International Scientific and Practical Conference* (pp. 72–73).

21. Teremetskyi, V. I., & Bernatskyi, O. V. (2026). Ecological safety of Ukraine: key challenges and critical factors of modern era. *Environmental law*, 1, 41–48. https://doi.org/10.37687/2413-7189.2026.1.6

22. Honcharuk, V., Parakhnenko, V., & Pidlisnyi, Ye. (2025). Pravovi ta upravlinski mekhanizmy ekolohichnoi bezpeky: Zakhyst navkolyshnoho seredovyshcha Ukrainy v umovakh viiny ta klimatychnykh vyklykiv. *Natsionalni interesy Ukrainy*, 10(15). https://doi.org/10.52058/3041-1793-2025-10(15)-922-929

23. Lyzun, M., & Ozarko, K. (2023). Economic security of the EU and Ukraine: new challenges and threats. *Vìsnik Marìupol's'kogo Deržavnogo Unìversitetu Serìâ Ekonomìka*, 13(25), 117–127. https://doi.org/10.34079/2226-2822-2023-13-25-117-127

24. Nikoliuk, O. V., Lahodiienko, N. V., & Demchenko, A. M. (2024). Sustainable development of Ukraine's national economy: *Challenges, risks and prospects.* Zenodo. https://doi.org/10.5281/zenodo.14876590

25. Madzhd, S. M. (2023). Sustainable development of Ukrainian society under war conditions: Ecological and economic aspects. *Institutional Repository of National University of Food Technologies*.

26. Sahaidak, I. (2025). Environmental challenges as a factor in the formation of modern economic policy. Humanities studies, 25(102), 138–146. https://doi.org/10.32782/hst-2025-25-102-15

27. Malysheva, N. (2025). Multidimensional challenges and threats: A test and stimulus for environmental lawmaking in Ukraine. Pravo Ukrainy, 8, 12. https://doi.org/10.33498/louu-2025-08-012

28. Filho, W. L., Fedoruk, M., Eustachio, J. H. P. P., Splodytel, A., Smaliychuk, A., & Szynkowska-Jóźwik, M. I. (2024). The environment as the first victim: The impacts of the war on the preservation areas in Ukraine. *Journal of Environmental Management*, 364, 121399. https://doi.org/10.1016/j.jenvman.2024.121399

29. European Parliament, & Council of the European Union. (2003, October 13). Directive 2003/87/EC of the European Parliament and of the Council establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC. Official Journal of the European Union, L 275, 32–46. http://data.europa.eu/eli/dir/2003/87/oj

30. European Parliament & Council of the European Union. (2000, June 29). Regulation (EC) No 2037/2000 on substances that deplete the ozone layer. Official Journal of the European Communities, L244, 1–24. http://data.europa.eu/eli/reg/2000/2037/oj

31. European Parliament, & Council of the European Union. (2006, May 17). Regulation (EC) No 842/2006 of the European Parliament and of the Council on certain fluorinated greenhouse gases (Text with EEA relevance). Official Journal of the European Union, L161, 1–11. https://eur-lex.europa.eu/eli/reg/2006/842/oj/eng

CHAPTER 3

UKRAINE'S ECONOMIC SECURITY WITHIN THE FRAMEWORK OF EUROPEAN ECONOMIC STABILITY



3.1. Strategic Guidelines for the Economic Security of the European Union

The current understanding of the European Union's economic security is shaped by the transformation of the international economic environment, intensifying geopolitical rivalry, the fragmentation of global economic links and the acceleration of technological change [1]. Open, rules-based trade has shaped the EU and benefited it since its inception. At the same time, rising geopolitical tensions and intensified geostrategic and geo-economic competition, as well as shocks such as the COVID-19 pandemic and the aggressive, large-scale war against Ukraine, have highlighted the risks inherent in certain forms of economic dependence [2]. Such risks, if not properly managed, could make it impossible to ensure the EU's economic resilience and the realisation of its strategic interests.

Under these circumstances, the traditional model in which economic openness was viewed primarily as a source of growth and increased efficiency is being supplemented by requirements for resilience, the autonomy of critical capabilities, and the European Union's ability to counter external economic influences [3]. In EU strategic documents, this transformation is reflected in a shift from a predominantly liberalisation-based approach to a model of "open strategic autonomy" [4–6], which aims to preserve the benefits of international economic integration whilst simultaneously reducing critical dependencies and enhancing the EU's capacity to act independently in areas of strategic importance.

On this basis, the EU's main strategic objective at the current stage of its development is to maximise the benefits of its economic openness whilst minimising the risks arising from economic interdependence, by establishing a common strategic framework for the EU's economic security. In contrast to the traditional understanding of security as primarily a military-political category, the EU's economic security takes the form of a comprehensive, cross-sectoral construct encompassing the trade, investment, technology, resource and infrastructure components of the single market's functioning [7].

The institutional foundation of the Union's current economic security architecture is the Joint Communication from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy "On the European Economic Security Strategy" of 20 June 2023 [4]. This document, for the first time at

a supranational level, established a holistic vision of economic security as a tripartite system of objectives (Fig. 3.1), which entails: firstly, strengthening the competitiveness and industrial potential of the European Union; secondly, protection against risks threatening this competitiveness; and thirdly, the development of partnerships with a wide range of countries interested in preserving an open, rules-based international economic order.

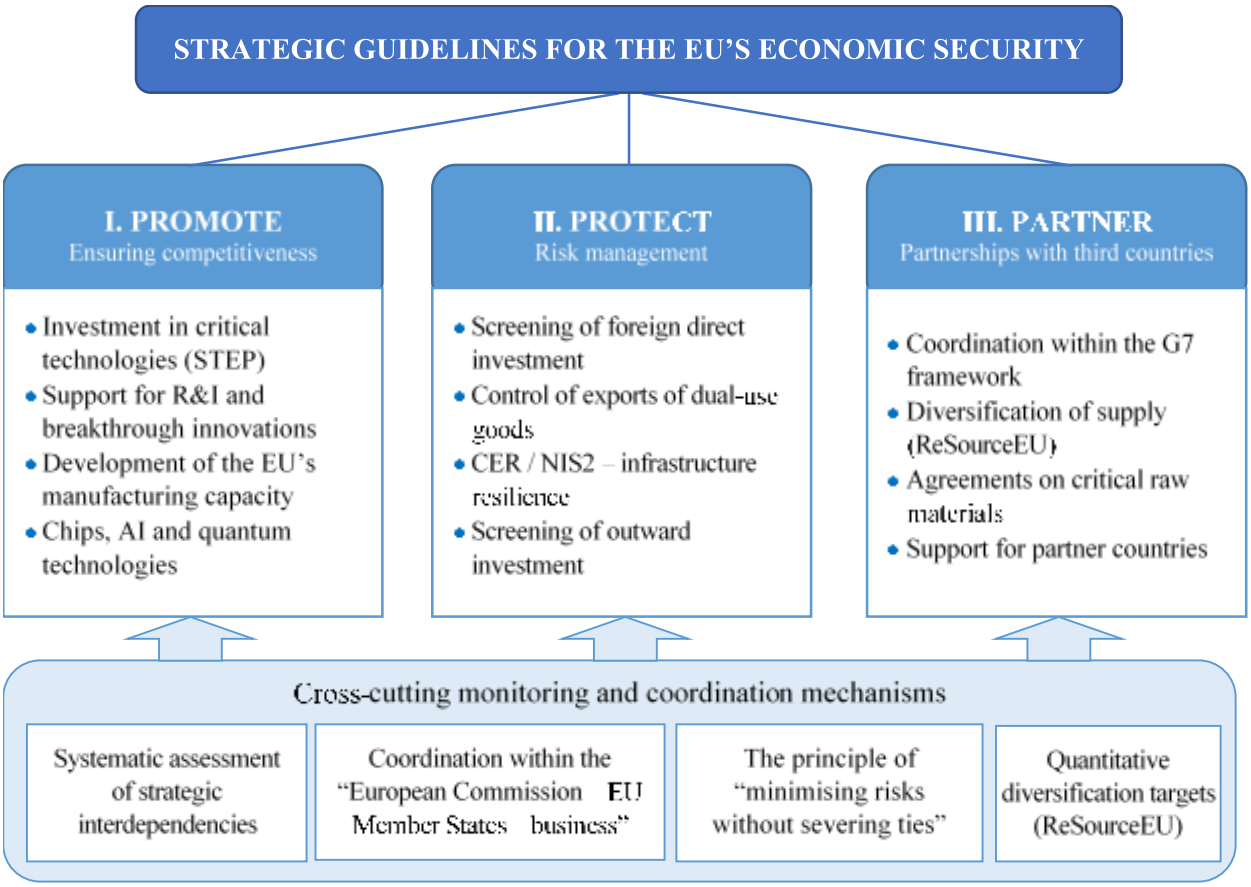


Fig. 3.1. Strategic guidelines for the EU's economic security
Source: compiled on the basis of [1–8]

The first priority involves strengthening the EU's internal economic capacity by developing competitiveness, the single market, and its scientific, technological and industrial base. This involves developing a competitive industrial sector, supporting research and innovation, strengthening the technological base, deepening the single market and creating the conditions for investment in strategic sectors [8]. This approach means that economic security is becoming increasingly linked to economic competitiveness: insufficient manufacturing, technological or innovative capacity creates the conditions for external dependencies to arise, which may subsequently turn into security risks. To this end, instruments are used to support investment in critical and breakthrough technologies [9], to stimulate research and innovation whilst

upholding the principle of openness in scientific and technological cooperation [10–12], and to develop production capacities in strategically important technological ecosystems [13], particularly in the fields of semiconductors, artificial intelligence, quantum technologies and biotechnologies.

According to data from the European Investment Bank [14], between 2015 and 2025, the real corporate investment index in the EU rose from 81 to 100 points (Q4 2019 = 100) (Fig. 3.2). Following a significant decline in 2020 due to the COVID-19 pandemic, investment activity gradually recovered, reaching a level close to pre-crisis levels in the third quarter of 2025.

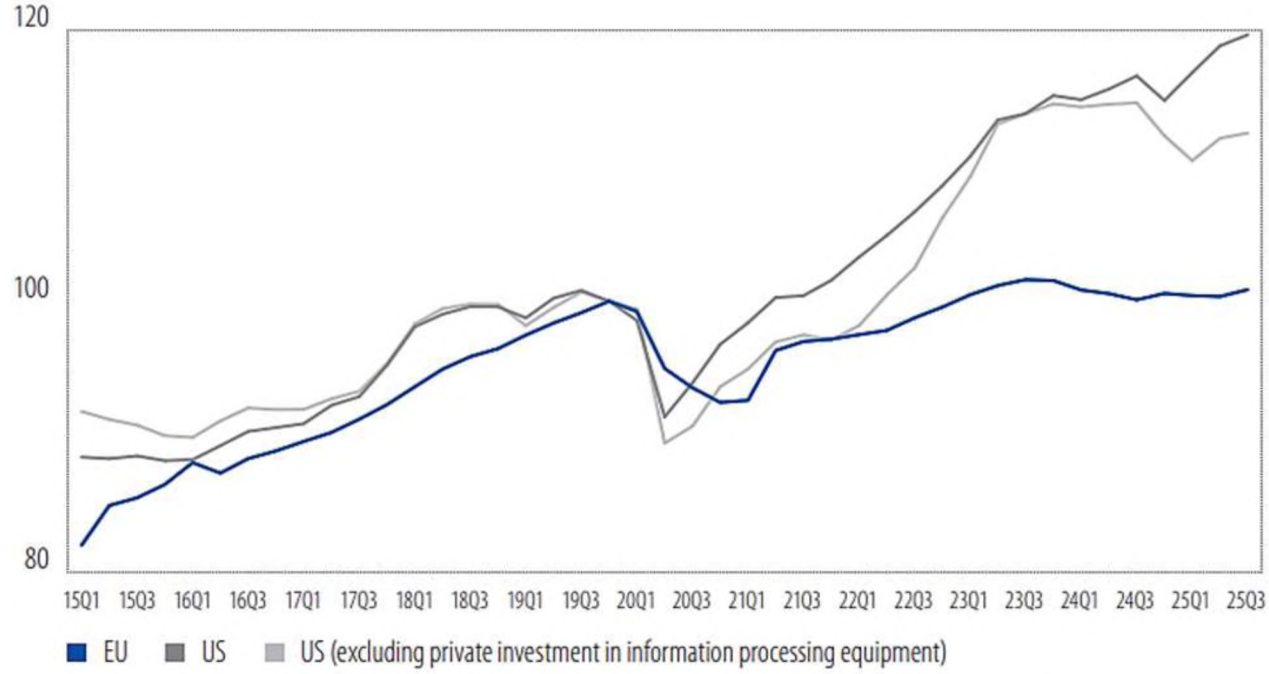


Fig. 3.2. Real corporate investment (index, 2019Q4=100)

Source: EIB staff calculations based on Eurostat and Federal Reserve economic data (FRED) [14]

The positive trend in corporate investment in the EU lays the foundation for strengthening its manufacturing and technological capabilities, however, a comparison with the US highlights the need to further increase investment specifically in strategically important technological sectors, as over the same period the index of real corporate investment in the US rose from approximately 88 to 119 points [14]. As shown in Fig. 3.2, a particularly marked acceleration was observed in 2023–2025, largely due to investment in information processing equipment. In the third quarter of 2025, this component of US private investment grew by 26 per cent year-on-year.

The importance of technology-oriented capital investment for strengthening economic and technological capacity is also underlined by the fact that, according to an EIB study [14] based on UN Comtrade data [15], between 2017 and 2024 global

exports of clean technologies rose by approximately 84 per cent, US exports by 23 per cent, whilst EU exports rose by 42 per cent and intra-European trade in such goods by 71 per cent (Fig. 3.3).

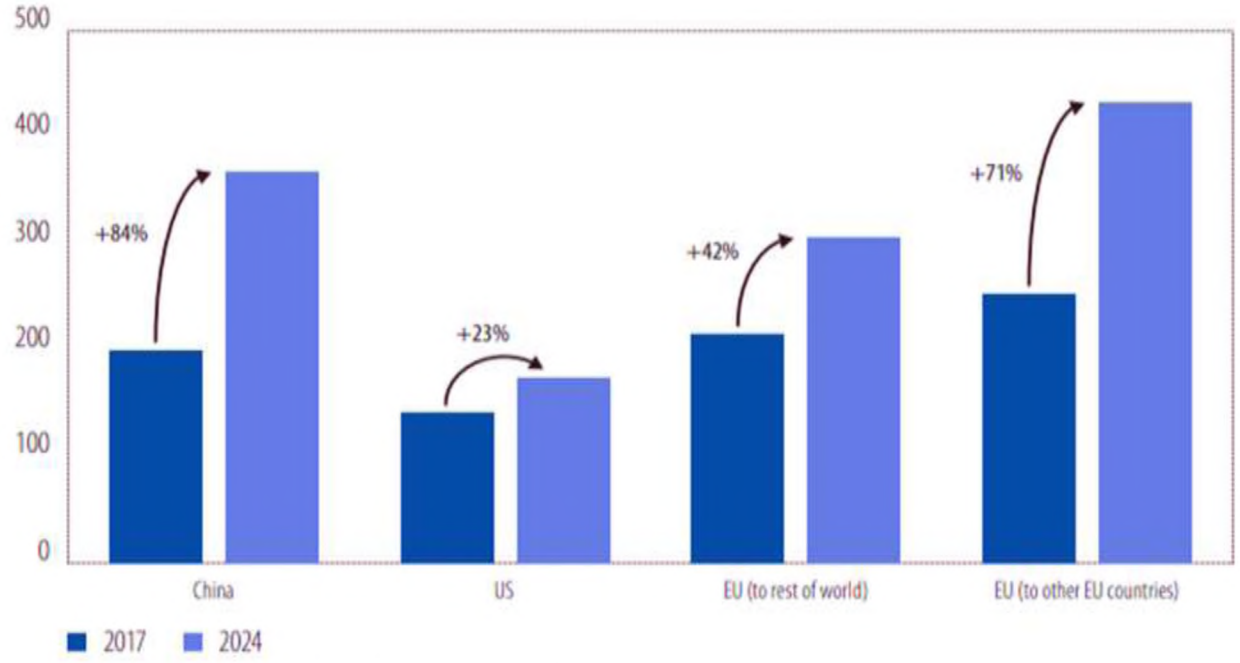


Fig. 3.3. Exports of cleantech goods ($ billion)
Source: EIB staff calculations based on UN Comtrade data [14]

This trend highlights the growing role of the EU single market in scaling up the production of clean technologies and, at the same time, underscores the need for continued support for innovative capacity, production capacity and domestic supply chains as key components of the Union's economic resilience.

The second strategic pillar of the EU's economic security relates to protecting the EU's economic space from targeted external risks through regulatory, trade, investment and technological instruments. In EU strategic documents, the emphasis is shifting from seeking to eliminate all dependencies to managing them in a differentiated manner [4–6]. Economic interdependence is not in itself regarded as a negative phenomenon, as risk arises when dependence becomes critical, is concentrated in a strategically important sector, and limits the EU's ability to respond to external pressure [16]. Trade, investment, technological, financial and resource links can be used not only for mutual economic benefit, but also to exert political or economic pressure. In this context, it is important to protect the EU's economic space from the use of economic dependencies as a tool of external influence [17].

The EU's external economic interdependencies are assessed using the EU Strategic Engagement Index, presented by the European Investment Bank in its Investment Report 2025/26 [14]. The index ranges from 0 to 1 and summarises the

significance of individual countries for the EU's strategic interests across components such as mutual trade, the depth of trade agreements, the share of investment by European companies, energy security, the supply of critical raw materials, participation in the EU's strategic corridors and the Global Gateway initiative, as well as political alignment.

According to the EIB's assessment [14], among 178 countries, Ukraine (1.0), Turkey (0.9), Bosnia and Herzegovina, Serbia and Moldova (0.8) have the highest index values, whilst Albania, Kosovo, Montenegro, North Macedonia, Georgia and Algeria have a score of 0.7 (Fig. A.1 in Appendix A). At the same time, over 40 per cent of the foreign trade of the Western Balkan countries, Ukraine, Moldova, Georgia and the countries of North Africa is with the EU, which indicates a concentration of strategically important economic ties in specific geographical directions.

It is advisable to monitor the EU Strategic Engagement Index on a regular basis as part of a system for the early detection of the EU's external economic risks, combining its values with indicators of trade dependence, supply concentration, energy and technological dependence, foreign direct investment flows and access to critical raw materials. It is particularly important to track the gap between a country's strategic significance and the actual dynamics of economic ties. According to EIB data [14], between January and July 2025, EU companies lost part of their market share in a number of strategically important candidate countries, notably Ukraine, North Macedonia and Kosovo, as well as Morocco, Lebanon and Algeria. Therefore, an increase or decrease in the index should not be viewed in isolation, but in conjunction with changes in trade and investment flows, as high strategic engagement coupled with a simultaneous weakening of the EU's economic presence may indicate a need to strengthen diversification and economic engagement tools, whilst excessive concentration of critically important links creates potential dependencies that could be transformed into a tool for external economic influence.

At the same time, EU policy focuses on the systematic, evidence-based assessment of the EU's strategic dependencies within sensitive industrial ecosystems, followed by a thorough investigative and analytical verification of the findings, the diversification of supplies, expanding the range of partners, developing domestic capabilities and establishing alternative channels of access to critical resources. This approach has been particularly evident in energy policy, policy on critical raw materials and strategic technologies.

The policy instruments in this area include mechanisms for screening foreign direct investment, controls on the export of dual-use goods, as well as countering economic coercion and protecting the domestic market from practices that create unequal competitive conditions [7].

The trend in EU imports between 2017 and 2024 [18] indicates a growing role for intra-European supply chains, particularly for goods that do not contain vulnerable

components. For this group, the rate of change in import trends from within the European Union and from outside it for dependent and independent goods rose from approximately 0.18 percentage points in 2017 to 0.81 percentage points in 2024, whereas for products containing vulnerable resources, the increase was more moderate – ranging from around -0.04 to 0.24 percentage points (Fig. 3.4). At the same time, for goods whose production is under-represented in the EU, the indicator remained close to zero throughout the period, and in 2022 it turned negative (-0.03 percentage points).

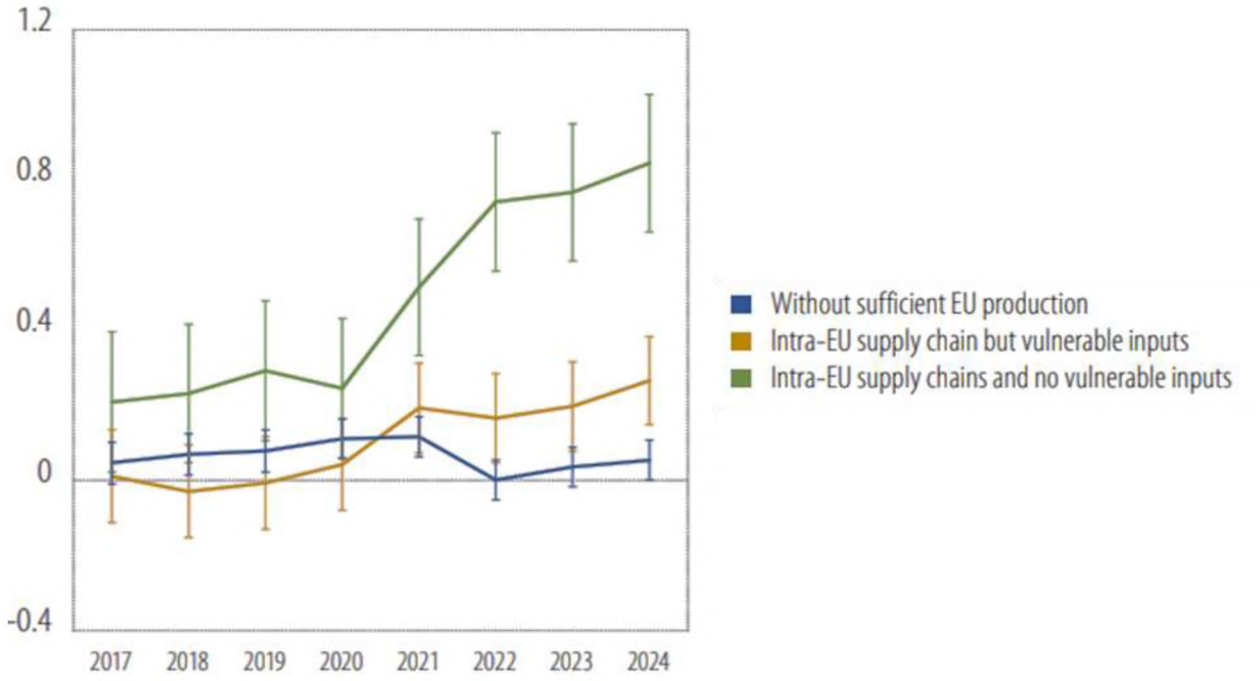


Fig. 3.4. Changes in the evolution of imports from within and beyond the European Union for dependent and non-dependent products (estimated coefficient, in percentage points)

Source: EIB staff calculations based on Comext [14]

The data presented illustrate a gradual shift in import flows towards intra-European supply chains, which is particularly pronounced in segments without critical dependencies, whilst imports of goods where the EU's domestic production capacity is limited remain more dependent on external sources.

In January 2024, the European Commission presented an additional package of measures as part of the implementation of the Economic Security Strategy [5, 10, 19–22], specifically regarding the improvement of controls on foreign investment, the monitoring of outward investment, export controls and the security of research activities.

Under its second strategic priority, the European Economic Security Strategy identifies the physical and cyber security of critical infrastructure, as well as technological security and the risks of technology leakage, as distinct categories of economic risk. This reflects a structural shift in the nature of economic security, as economic resilience increasingly depends on digital networks, data, high-tech production systems, scientific research and infrastructure facilities, the disruption of which can have simultaneous economic, social and security consequences [23–25].

The technological dimension of economic security is of particular importance. In 2023, the European Commission identified four technological areas of critical importance to the EU's economic security: advanced semiconductor technologies, artificial intelligence, quantum technologies and biotechnologies [4]. Their identification signals a shift towards preventive management of technological risks [26], where strategic importance is attached not only to the current competitiveness of a particular technology, but also to the potential impact of its concentration, uncontrolled transfer or dependence on external suppliers on the EU's future autonomy.

The third strategic pillar of the EU's economic security involves deepening cooperation with states and international partners to diversify economic ties and sources of supply for critical raw materials, establish interdependencies at an acceptable level of risk, and respond jointly to transnational threats [7].

A chronological comparison of EU strategic documents in the field of economic security (Table 3.1) reveals a consistent trajectory of transition from fragmented, sector-specific protection measures (investment screening) to a comprehensive economic security strategy for 2023, and subsequently to a quantitatively verifiable, operational model with defined targets and timeframes for their achievement (2024–2026). In 2025, the European Commission further strengthened its focus on a risk-based approach and a more proactive use of existing economic security instruments.

Thus, ensuring the EU's economic security involves not only protection against external threats, but also the simultaneous internal strengthening of the economic base, the management of external dependencies and the development of a network of international partnerships. This framework is of fundamental importance, as the EU's resilience is viewed not only as the ability to respond to threats that have already materialised, but above all as the capacity to prevent excessive dependencies, diversify sources of resources and technologies, and preserve freedom of economic choice. The EU's concept of economic security is shifting from a reactive defence of economic interests to the proactive management of strategic dependencies, risks and vulnerabilities.

Table 3.1

A comparative analysis of the EU's strategic priorities for economic security and the measures for their implementation during 2019–2026

Strategic documents	Strategic guideline	Measures to implement strategic objectives
Regulation (EU) 2019/452 (FDI screening framework), 2019-2020	Proactive, sector-specific approach through control of access to the EU's strategic assets	National FDI screening mechanisms; the European Commission's coordination mechanism, over 1,000 agreements reviewed since October 2020
Joint Communication JOIN(2023) 20 final "European Economic Security Strategy", June 2023	Introduction of the Promote-Protect-Partner triad; the principle of "de-risking, not decoupling"	Mandate to identify a list of critical technologies, launch of an assessment of strategic dependencies, initiation of a review of the FDI screening framework
Instrument against Economic Coercion, Regulation (EU) 2023/ 2675, December 2023	Operationalisation of the Protect pillar: the capacity to respond to economic pressure from third countries	Procedure for establishing the existence of coercion, the EU's arsenal of countermeasures (trade, investment and regulatory)
European Economic Security Package, January 2025	Detailed methodology: risk assessment of critical technologies and research security	A joint list of four critical technology sectors, recommendations on export controls and screening of outward investment
Regulation on Critical Raw Materials, (EU) 2024/1252 (CRMA); STEP Platform, (EU) 2024/795	Operationalisation of the Promote pillar: reducing resource and production dependence	Quantitative targets for the extraction/processing of critical raw materials in the EU, reallocation of financial instruments towards critical technologies
Joint Communication on Strengthening the EU's Economic Security; ReSourceEU Action Plan, December 2025	A paradigm shift from a reactive to a proactive, systemic model for the application of instruments	Quantitative targets for supply diversification (30–50 per cent by 2029 for batteries, rare earths and defence-critical materials), 12- and 36-month deadlines
Implementation phase of the Directive on the Resilience of Critical Entities (CER), (EU) 2022/2557, January 2026	Operationalisation of the Protect pillar at national level	Deadline for Member States to submit risk assessments of critical infrastructure (17 January 2026)

Source: compiled on the basis of [4–13, 19–22, 27]

The proposed strategy establishes a common framework for achieving economic security by strengthening the EU's economic base and competitiveness, safeguarding against risks, and partnering with as wide a range of countries as possible to address shared challenges and interests (Fig. 3.5).



Fig. 3.5. Conceptual chart illustrating the implementation of the EU's strategic economic security objectives

Source: compiled from [4–13, 19–22]

Measures to ensure economic security are based on the fundamental principles of proportionality and precision, and are consistent with the EU's interests and values: the rule of law, human rights, and international norms and standards [7]. Thus, ensuring the EU's economic security is based on ongoing risk assessments and strategic coordination with Member States to achieve a common understanding of the risks facing the EU and how to respond to them.

The EU's economic security strategy provides for the following key measures [4, 7]:

– to develop, together with Member States, a framework for assessing risks affecting the EU's economic security; this includes drawing up a list of technologies that are critical to economic security and assessing the risks associated with them, with a view to developing appropriate mitigation measures;

– engage in a structured dialogue with the private sector to develop a shared understanding of economic security and encourage them to carry out due diligence and manage risks in the light of economic security concerns;

– continue to support the EU's technological sovereignty and the resilience of value chains within the EU, including through the development of critical technologies via the Strategic Technologies for Europe Platform (STEP);

– review the Foreign Direct Investment Screening Regulation;

– explore options for providing adequate targeted support for research and development of dual-use technologies;

– fully implement the EU Export Control Regulation on dual-use goods and put forward proposals to ensure its effectiveness and efficiency;

– examine, together with the Member States, what security risks may arise as a result of foreign investment;

– to propose measures to improve research security, ensuring the systematic and rigorous application of existing instruments, as well as identifying and addressing any remaining gaps;

– examine the targeted use of Common Foreign and Security Policy (CFSP) instruments to strengthen the EU's economic security, including hybrid and cyber diplomacy toolkits and toolkits addressing foreign information manipulation and interference (FIMI);

– task the Single Intelligence Analysis Centre (SIAC) with working specifically to identify potential threats to the EU's economic security;

– ensure the full integration of the protection and promotion of the EU's economic security into the European Union's external action and step up cooperation with third countries on economic security issues.

Of fundamental importance is the methodology of "de-risking, not decoupling", which is of fundamental importance. This methodology signalled the EU's departure

from both the policy of unrestricted economic openness characteristic of previous decades and from protectionist isolation, whilst at the same time outlining an intermediate, balanced trajectory for the selective reduction of vulnerabilities in clearly defined critical areas [4].

This approach was further institutionalised within the 2024 European Economic Security Package, which set out in detail the tools for assessing strategic dependencies [19–22], as well as in the Joint Communication of 3 December 2025, which marked a shift from a predominantly reactive to a systematic, proactive model for applying the tools at the EU's disposal, regardless of their original functional purpose [6]. An integral part of this updated approach was the ReSourceEU Action Plan, aimed at overcoming the Union's excessive dependence on imports of critical raw materials, setting quantitative targets for supply diversification (in the range of 30–50 per cent by 2029 for specific categories of critical raw materials, in particular battery and rare-earth materials) [27].

The European Union is responding to the challenges posed by geopolitical and technological changes through a comprehensive system of regulatory initiatives that combines strategic planning, proactive monitoring and coordination between Member States and the private sector. For Ukraine, these approaches can serve as a guide when improving national legislation in the field of economic security, enabling the integration of European experience in strategic planning for collective security.

The EU pays particular attention to the control of foreign investment, which, on the one hand, contributes to economic development, but on the other, may pose risks to security and public order. Based on an analysis of over a thousand foreign direct investment transactions, the European Commission has drawn up a proposal to improve the screening system [19], which provides for the harmonisation of national rules, the definition of a minimum sectoral scope for screening, and the extension of controls to investments made through entities owned by investors from third countries.

At the same time, the EU is stepping up the monitoring and assessment of outward investments, particularly in a narrow range of cutting-edge technologies that could enhance the military or intelligence capabilities of third-country entities. The White Paper on Outbound Investments [20] proposes a phased analysis of such investments, involving three-month consultations and 12-month monitoring at national level, ensuring a joint assessment of risks and the determination of the appropriateness of policy measures.

Growing geopolitical complexity is also prompting the EU to coordinate export controls on dual-use technologies, such as advanced electronics, toxins, nuclear and missile technologies, in order to prevent their use to undermine security or violate human rights. The EU's Common Control List [21] and a high-level forum for

coordinating national lists ensure coherence and prevent fragmentation at national level.

The European Union also actively supports research and development into technologies with dual-use potential, by integrating civil and defence funding programmes and considering the creation of specialised instruments to support strategic R&D. The White Paper on options for enhancing support for research and development involving technologies with dual-use potential [22] stimulates public consultation, enabling public authorities, industry, research institutions and civil society to be involved in determining the next steps.

In the context of open international scientific and innovation cooperation, the EU pays particular attention to research security, as the results of scientific activity may be used for military purposes or undermine fundamental values. Higher education institutions and research organisations are protected against malicious influence from third countries, whilst the Council's recommendations ensure that measures are coordinated at both Union and Member State level [10].

The implementation of such approaches enables the development of an economic security system capable of responding effectively to contemporary threats, integrating national interests into the European collective security system, and enhancing the state's resilience in complex geopolitical and technological conditions [28]. The key components of such a comprehensive improvement are: the legislative enshrinement of transparent procedures for the assessment and control of strategic investments; the integration of preventive risk assessment mechanisms; the establishment of uniform approaches to the control of dual-use technologies; and the safeguarding of scientific and technical cooperation.

Thus, the 2023 European Economic Security Strategy [4] has effectively established a comprehensive framework for identifying, assessing and minimising economic risks that may affect the EU's security, competitiveness and strategic interests. At the same time, the European approach does not, in principle, envisage the isolation of the internal market. On the contrary, a key strategic premise is the preservation of the EU as an open and attractive space for trade, investment, entrepreneurship and technological development, provided that risk management is more targeted.

The evolution of the European Union's strategic economic security guidelines reflects a gradual transformation of supranational economic policy from a predominantly market-liberalisation paradigm to a model of managed openness, in which market access is increasingly contingent upon compliance with economic security criteria. The key feature of this transformation is the shift from a reactive, ad hoc application of individual instruments to a systematic, cyclical model of risk management that integrates the analytical assessment of interdependencies, the

selection and application of regulatory instruments, and multi-level coordination. This lays the foundations for further academic analysis of the institutional, legal and economic consequences of such a transformation, particularly in the context of the adaptation challenges facing third countries, with whom the European Union declares its partnership to be an integral element of its economic security.

3.2. Threats to Ukraine's economic security in the context of war and European integration

Traditional approaches to ensuring Ukraine's economic security were shaped primarily against a backdrop of relative stability in the international environment, the predictability of global economic processes and the stability of inter-state economic ties. The intensification of geo-economic contradictions and structural changes in the global economy necessitate the adaptation of national economic systems to operate in conditions of high uncertainty [29, 30]. Military, economic and hybrid challenges and threats highlight the need to update approaches to ensuring the state's economic security, focusing them primarily on the early detection and timely consideration of new risks [31].

In this context, it is of great importance to systematically monitor the key trends, factors and destructive processes that determine the dynamics of socio-economic development, as well as to refine methodological tools for identifying and assessing risks, taking into account their interdependence and multidimensional nature. The establishment of effective mechanisms to counter and minimise threats to economic security is a necessary prerequisite for maintaining the resilience of the economy in wartime and for creating the institutional and economic foundations for its subsequent recovery [32]. This takes on particular significance in the context of deepening Ukraine's economic integration with the European Union and aligning national mechanisms for ensuring economic security with European approaches.

At the international level, experts from the World Economic Forum systematically conduct the Global Risks Perception Survey (GRPS) [33], which provides the information base for ensuring sustainable economic development. In this survey, a global risk is defined as the possibility of an event or condition occurring which, if it were to happen, would have a negative impact on a significant proportion of global GDP, the population or natural resources [33]. Given the interconnection and interdependence of risks, global risks give rise to risks at lower levels of the social hierarchy (at the level of regions, states and economic actors). In turn, lower-level risks can act as catalysts for higher-level risks [34] (Fig. 3.6).



Fig. 3.6. Sources of threats to economic security

To ensure the timely identification of and appropriate response to destabilising factors that may pose a threat to economic security, an annual assessment and categorisation of key global risks is carried out at a global level as part of the Global Risks Perception Survey (GRPS) [33] is carried out annually across three time horizons: one, two and ten years, enabling the identification of potential threats and the formulation of appropriate measures to neutralise or minimise them.

The Global Risks Report 2026 identifies 33 global risks across five categories (Economic, Environmental, Geopolitical, Societal and Technological). Their ranking by level of risk in the short term (2 years) and long term (10 years) is shown in Fig. 3.7.

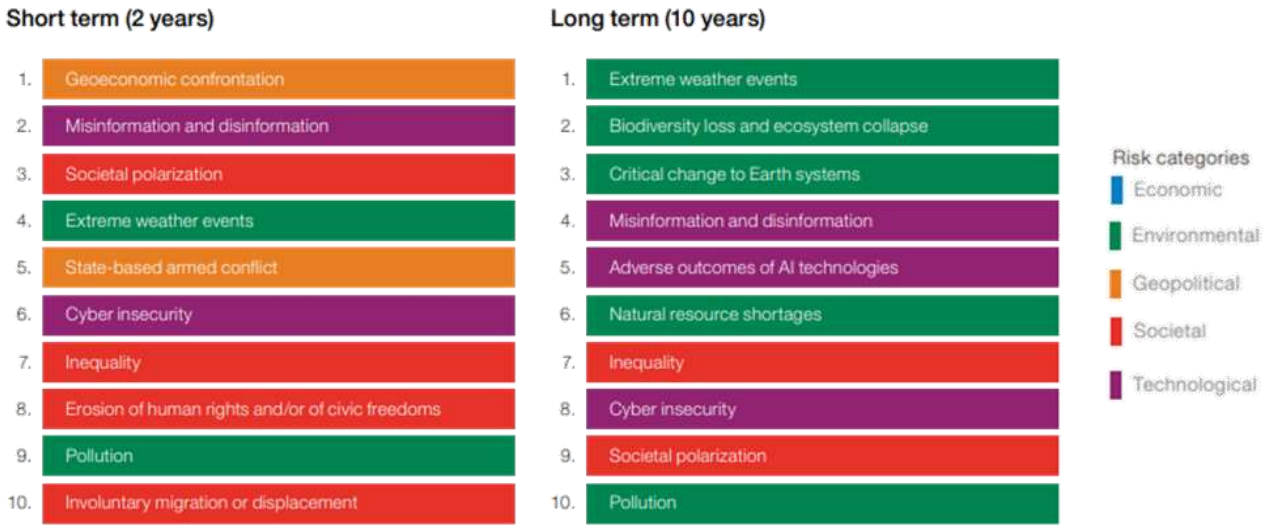


Fig. 3.7. Global risks ranked by severity

Source: World Economic Forum Global Risks Perception Survey 2025-2026 [33]

According to experts, contemporary global risks do not exist in isolation: political, economic, social, environmental and technological threats are becoming increasingly intertwined, reinforcing one another and creating complex chains of interactions and a high level of danger for the global community [35, 36] (Appendix B). This requires political leaders and analysts to adopt holistic, interdisciplinary approaches to risk assessment and the development of response strategies capable of enhancing the resilience of national economies and societies in the face of growing global turbulence.

In the short term (up to 2027), according to the Global Risks Report 2026, the most dangerous risk to global stability is geo-economic confrontation (Fig. C.1 in Appendix C), which ranks highest among the threats and is linked to existing and potential new areas of tension. Such factors are capable of causing significant disruptions to global production and financial chains, reducing investment activity and hindering international cooperation [37].

In addition, in the short term, social polarisation and information risks are attracting significant attention, in particular the spread of disinformation and manipulative narratives, which deepen divisions within societies and undermine trust in political and economic institutions [38]. These phenomena can exacerbate conflicts, intensify economic imbalances and hinder the effective coordination of international responses to crises.

According to the World Economic Forum, long-term global challenges (up to 2036) are predominantly environmental in nature, the most dangerous of which are extreme weather events, biodiversity loss and ecosystem collapse, and critical changes in Earth's systems, which place long-term pressure on food security, resources and economic stability across various regions [39]. These risks are closely interlinked with climate change and may have implications for international trade, infrastructure, the insurance sector and human health.

A distinct range of risks is posed by cutting-edge technologies, in particular AI and quantum technologies, the development of which alongside potential economic and social benefits may intensify technological competition, economic fragmentation and geopolitical tensions [40–42]. Technological risks are becoming increasingly complex, as their impact extends simultaneously to the economic, social, information and security spheres and is linked to the transformation of labour markets, the spread of disinformation, cyber threats, the negative consequences of the use of artificial intelligence, and so on.

Another important dimension of contemporary global risks is socio-economic risks, in particular threats linked to demographic changes, inequality, a slowdown in economic growth and potential financial shocks. Even if some economic risks may not feature among the most pressing in the short term, their interaction with political and

environmental factors has a significant impact on the resilience of states and societies (Fig. 3.8).

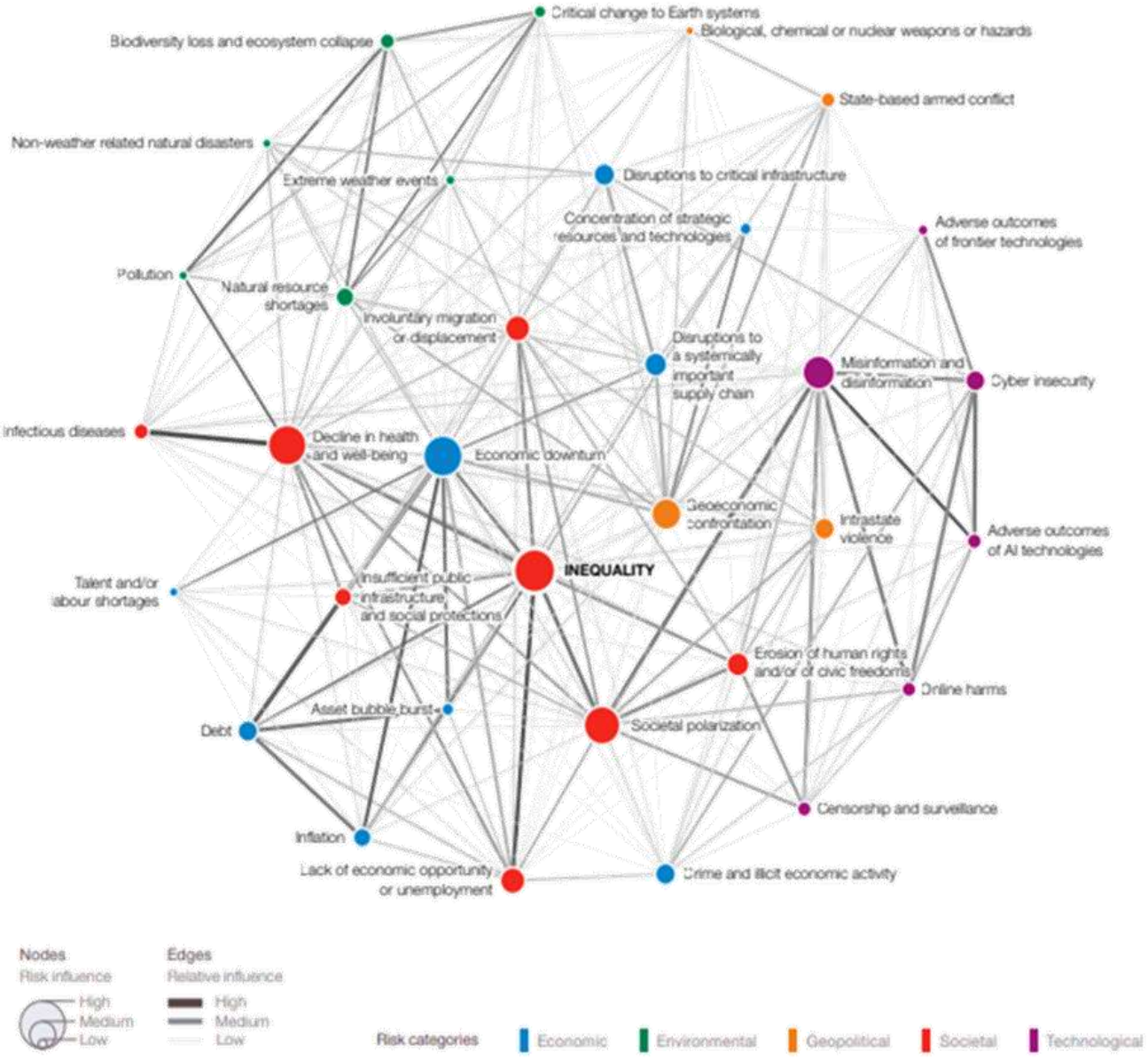


Fig. 3.8. Interactions between the most dangerous global risks according to the GRPS 2026

Source: World Economic Forum Global Risks Perception Survey 2025-2026 [33]

However, for Ukraine, which is directly affected by a large-scale war, the priorities regarding existing challenges are somewhat different; therefore, in the short term, the most serious threats to Ukraine's economic security are directly linked to large-scale military operations and attacks on critical infrastructure [33] (Fig. 3.9).

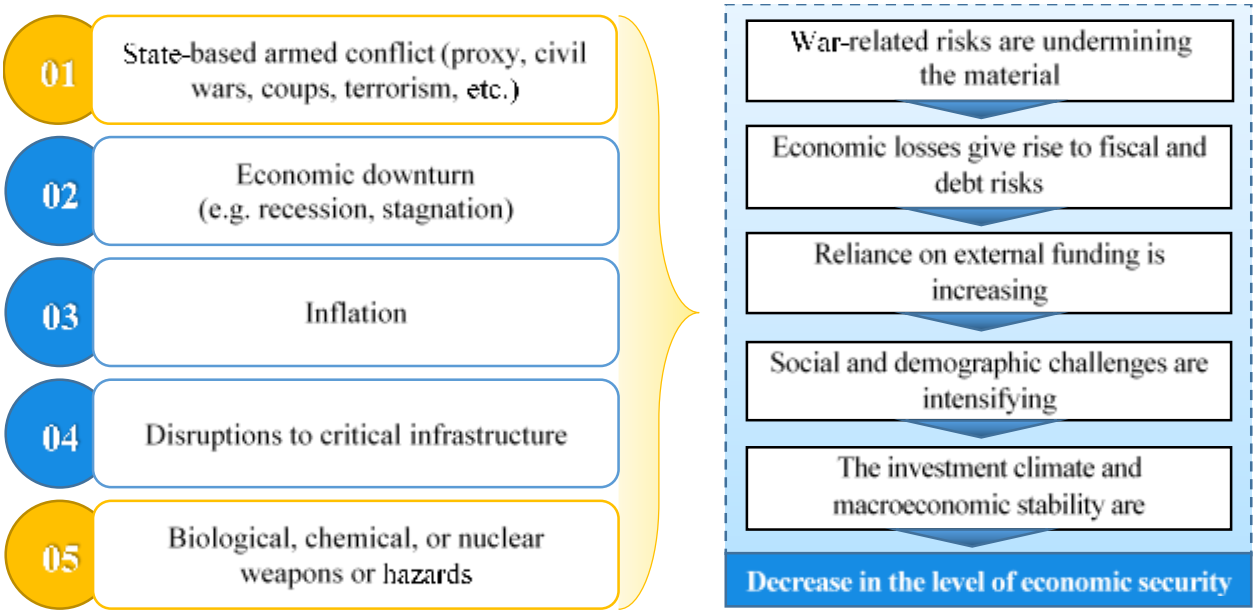


Fig. 3.9. The most serious risks to Ukraine according to the GRPS 2026 and their impact on the country's economic security

Source: compiled using data from the World Economic Forum's Global Risks Perception Survey 2025–2026 [33]

In the context of war, the main catalyst for risks in Ukraine is military attacks, which pose threats to the physical functioning of industrial, energy and transport infrastructure, human capital, foreign economic relations and the state's ability to provide critical public services [43] (Fig. 3.10).

The scale of the materialised military threats is confirmed by the findings of a joint assessment carried out by the Cabinet of Ministers of Ukraine, the World Bank, the European Commission and the UN [44–46]. According to RDNA5 data, as at 31 December 2025, direct losses from the war exceeded US$195 billion, whilst the total need for recovery and reconstruction over the next decade is estimated at nearly US$588 billion [46]. The housing, transport and energy sectors were the hardest hit. At the same time, the need for transport infrastructure recovery increased by approximately 24 per cent during 2025, whilst the number of damaged or destroyed energy assets rose by approximately 21 per cent [46].

A systemic threat to Ukraine's economic security in the context of military operations is the destruction of critical economic infrastructure (Fig. C.2 in Appendix C). This involves not only the loss of physical assets, but also the disruption of production, logistical and inter-sectoral links, an increase in transaction costs, a reduction in the supply of energy and transport services, and a greater dependence of the economy on external resources [47]. The cumulative nature of this threat is particularly dangerous (Fig. C.3 in Appendix C), as damage to energy infrastructure reduces industrial production capacity, disruption to transport links restricts exports and imports, and a decline in production activity, in turn, narrows the tax base and complicates the financing of reconstruction.

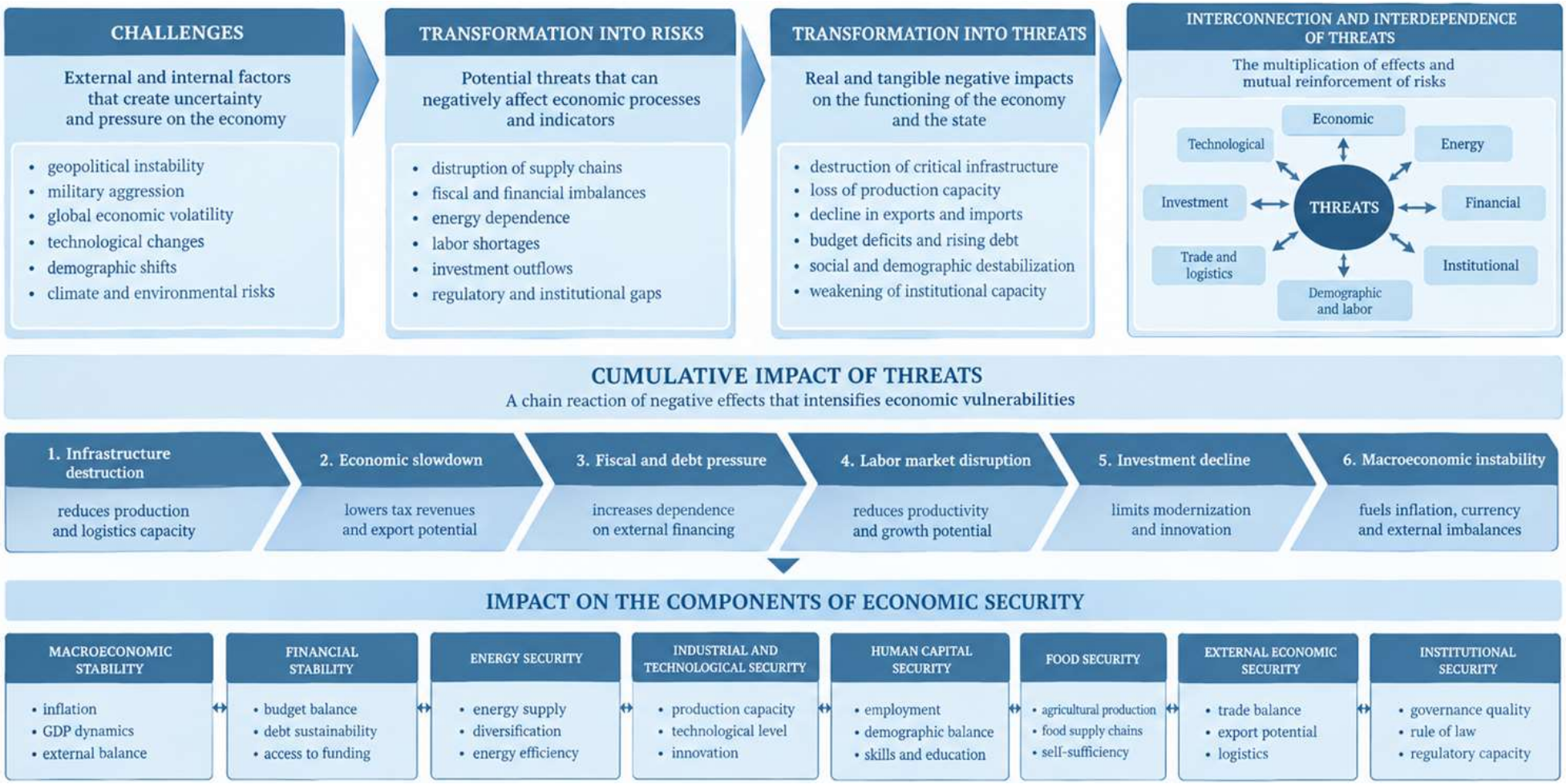


Fig. 3.10. A conceptual model of the process by which challenges are transformed into risks and threats to Ukraine's economic security, taking into account their interrelationships and interdependencies

Source: compiled from [1–8]

The energy component of economic security is of particular importance. Systematic attacks on power generation, transmission and distribution facilities pose a risk not only of temporary electricity shortages, but also of a long-term deterioration in operating conditions for industry and the service sector. International assessments indicate that energy infrastructure is among the sectors that have suffered the most extensive damage, and repeated attacks have a direct impact on Ukraine's economic dynamics [46].

The hostilities have exacerbated the demographic crisis in Ukraine, as evidenced by the decline and structural transformation of human capital. The war has led to large-scale internal and external population displacement, losses of human capital, the destruction of housing, the disruption of education, and a deepening of imbalances in the labour market. According to OECD estimates, approximately a quarter of Ukraine's population has been displaced as a result of the war, whilst the total scale of damage to or destruction of housing, businesses and infrastructure is estimated to be significantly higher than pre-war GDP [45]. From an economic perspective, this problem extends far beyond demographic statistics. The loss or prolonged absence of part of the working-age population means a reduction in the potential labour supply, a worsening shortage of skilled workers and an increase in businesses' costs for recruiting and training staff. The IMF, in particular, notes that the persistence of a significant labour shortage is one of the factors contributing to inflationary pressures and limiting production capacity [44].

Another fundamental threat is the increasing fiscal and debt vulnerability of the state. The protracted war is leading to a simultaneous rise in expenditure on defence, social protection, the reconstruction of damaged infrastructure and the maintenance of the public sector's operations, against a backdrop of limited domestic revenue. The International Monetary Fund emphasises that the continuation of the war is accompanied by significant budget deficits and a need for large-scale external financing. In particular, Ukraine's budgetary parameters for 2026 envisage the continuation of the war, which implies that significant fiscal needs will persist [44].

Accordingly, the fiscal threat has two dimensions. In the short term, it lies in the need to constantly mobilise substantial financial resources to cover the budget shortfall. In the long term, it lies in the need to ensure debt sustainability and a gradual transition from a model of crisis financing to one of self-sustaining economic growth. In this context, external financial support plays a stabilising role, whilst at the same time raising questions regarding the predictability of international aid, its conditionality, and Ukraine's ability to build up its own resource base.

The threat of war, damage to assets, logistical constraints, instability in energy supplies and uncertainty regarding the duration of the war are limiting the willingness of private capital to make long-term investments. This is particularly critical for

Ukraine, as the scale of reconstruction far exceeds the capacity of budgetary funding. RDNA5 estimates reconstruction needs at nearly US$588 billion [46], making the involvement of the private sector a prerequisite for long-term reconstruction.

At the same time, the investment risk is not only quantitative but also structural in nature. Ukraine's recovery will require not merely the restoration of pre-war production capacity, but the creation of a technologically modernised, energy-efficient and competitive economy. This is precisely why international partners link the reconstruction process to reforms, economic modernisation and alignment with EU standards [48]. The World Bank emphasises that investment in reconstruction must simultaneously support economic recovery, enhance resilience and contribute to Ukraine's progress towards EU membership [46].

The combined effect of these threats to Ukraine's economic security gives rise to macroeconomic imbalances, including inflationary risks, a foreign trade deficit, dependence on imports of critical goods and energy resources, and constraints on production capacity. According to IMF estimates, in 2025 Ukraine's real GDP remained approximately 20 per cent below its pre-war level [44], whilst economic growth was held back, in particular, by the consequences of attacks on energy infrastructure, labour shortages and other war-related shocks.

At the same time, the war significantly altered the geographical and commodity structure of Ukraine's foreign trade, and the blockage of traditional Black Sea logistics routes necessitated the re-routing of a significant portion of exports via land and river routes through the territory of EU Member States, with the aim of sustaining export revenues and replenishing Ukraine's state budget. In this context, the European Union's launch of 'Solidarity Lanes' [49] became one of the mechanisms for sustaining Ukrainian exports and imports amidst the disruption of traditional transport corridors.

At the same time, the deepening of trade and economic integration with the EU necessitates that Ukrainian manufacturers adapt to European technical, environmental, sanitary, phytosanitary and competition requirements. Consequently, integration into the single European economic area creates significant opportunities for Ukraine to expand its markets and attract investment, but at the same time raises the bar in terms of enterprises' technological standards, product quality and the effectiveness of the regulatory environment.

This aspect takes on particular significance in light of Ukraine's transition from the stage of political association to the actual process of EU accession. Ukraine officially obtained candidate status in June 2022, and accession negotiations were formally launched in June 2024. In September 2025, Ukraine completed the bilateral legislative screening, which involves a comprehensive assessment of the compliance of the Ukrainian regulatory framework with EU law [50].

Thus, in the current context, taking into account the multifaceted impact of global risks, the most dangerous threats to Ukraine's economic security are linked to the simultaneous impact of war and the processes of European integration. The cumulative impact of these threats is illustrated in Fig. 3.11.

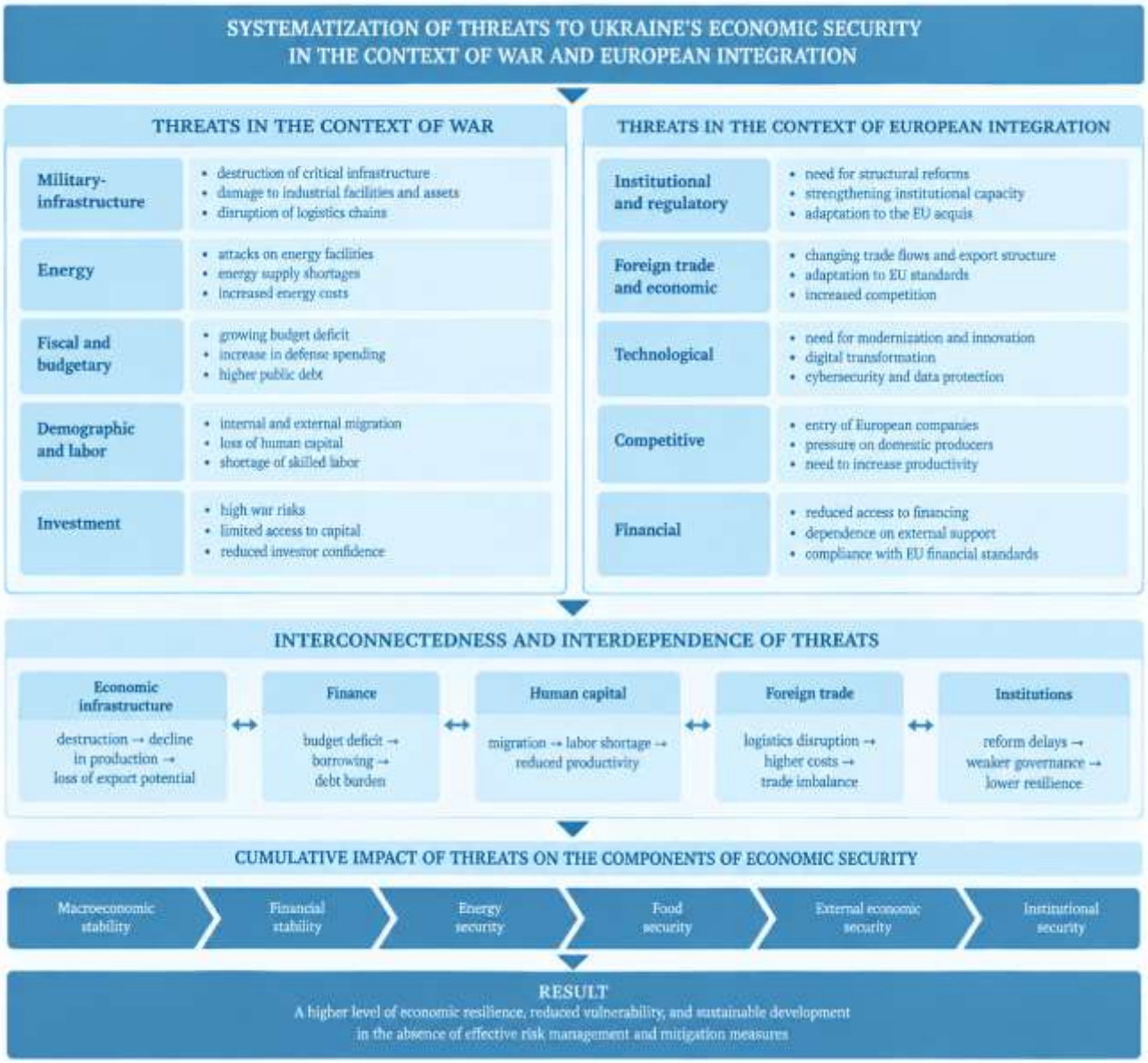


Fig. 3.11. The cumulative impact of threats on Ukraine's economic security in the context of war and European integration

Ukraine's deepening integration into the European economic and legal area gives rise to institutional and regulatory risks linked to the need to carry out large-scale structural reforms whilst the economy continues to function in a wartime environment.

European integration requires the strengthening of public administration, the rule of law, competition policy, corporate governance, the public finance system, anti-corruption

mechanisms and regulatory capacity. For Ukraine, the problem lies in the fact that these reforms are being implemented whilst state institutions are under an extremely heavy strain.

Consequently, it is appropriate to systematise the threats to Ukraine's economic security in the context of the war and European integration in Table 3.2.

Table 3.2

Systematisation and analysis of the impact of threats on Ukraine's economic security in the context of war and European integration

Threat category	Main manifestation	Potential impact on economic security
Military	Destruction of the energy sector, transport, housing and production assets	Reduction in production capacity and rising costs
Fiscal and debt	Significant budget deficit, growing financing needs	Increased dependence on external financial support
Energy	Damage to energy generation, transmission and distribution	Disruptions to production, dependence on imports, inflationary pressure
Demographic and labour	Migration, population displacement, labour shortages	Reduction in the labour force and productivity
Foreign trade	Logistical disruptions, changes to export routes	Deterioration in the balance of trade and rising transport costs
Investment	High war risks and uncertainty	Restrictions on private investment
Macroeconomic	Inflation, external imbalances, weak economic growth	Decreased economic stability and predictability
Institutional	Insufficient capacity to implement structural reforms	Slowing of modernisation and European integration
Regulatory	The need for large-scale alignment with EU law	Additional alignment costs for the state and business
Corruption	Risks of inefficient use of public resources	Declining confidence among investors and international partners

The mutual reinforcement of threats poses a particular danger. For example, the destruction of energy infrastructure reduces enterprises' production capacity, which in turn lowers tax revenues and export potential; a decline in exports worsens the balance of payments; a budget deficit increases the need for external financing; and uncertainty regarding security deters private investment. This gives rise to a cumulative mechanism for the reproduction of economic vulnerability, whereby individual threats cease to be isolated and become a systemic risk to economic stability.

Consequently, the key characteristic of contemporary threats to Ukraine's economic security is their systemic nature, interdependence and capacity for a cumulative effect. War directly destroys the material basis of economic activity, whilst simultaneously creating secondary fiscal, demographic, investment and foreign trade consequences. European integration, in turn, entails a large-scale institutional and

structural transformation of the economy. Therefore, the task of ensuring Ukraine's economic security lies not only in neutralising current threats, but also in shaping a model of economic development that will ensure resilience to external shocks, competitiveness in the European market, technological modernisation and the state's institutional capacity.

3.3. Forming an ecosystem of economic resilience to hybrid threats: European experience and opportunities for its implementation in Ukraine

The conceptual foundations of the EU's economic security are based on ensuring economic resilience to external and internal threats [7]. For Ukraine, in the context of a full-scale war, this paradigm takes on particular significance, as economic resilience becomes an essential prerequisite not only for economic development but also for maintaining the state's functional capacity.

The EU Global Strategy states that a resilient state is a secure state, and that security is the foundation of prosperity and democracy [52]. However, ensuring secure and sustainable development requires support for more than just state institutions. The document outlines a shift towards a broader approach understanding sustainability as a concept that encompasses all people and the whole of society, since a sustainable democratic society, characterised by trust in institutions, and sustainable development form the foundation of a sustainable state [52].

The current stage of societal development is characterised by the unprecedented scale of so-called hybrid threats, which combine various methods of influence ranging from economic pressure to information and psychological attacks and are aimed at undermining the stability of states and democratic institutions. Understanding the nature of these threats and applying effective mechanisms to neutralise them is becoming a key element of contemporary economic security policy, both within national systems and at the level of the EU as a whole.

Hybrid threats are characterised by a combination of overt and covert instruments of influence, which are used to achieve strategic objectives without official acknowledgement. Their primary targets are democratic institutions, governments and individual states, and their aim is to restrict the freedom of action of democracies, undermine public trust and create advantages for authoritarian regimes. The main channels through which they exert influence are: economic pressure, information campaigns, cyber-attacks and psychological manipulation, which enable them to influence social cohesion and public opinion [53].

The European Union and individual EU countries are actively developing systems to counter hybrid threats (Fig. 3.11). The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) [54], established in 2017, plays a key role in coordinating activities to analyse, assess and neutralise hybrid risks. Furthermore, EU countries are actively implementing programmes to enhance resilience to information, psychological and cyber-attacks, which include monitoring disinformation, developing media literacy, protecting critical infrastructure and strengthening coordination between government, business and civil society.

Historical and contemporary examples of hybrid threats demonstrate the very real danger they pose. Such examples include interference in elections and disinformation campaigns in the US and EU countries, economic and military pressure on Taiwan by China, and the Russian Federation's comprehensive actions against Ukraine prior to and during the full-scale aggression. To counter these threats, it is necessary to raise awareness of hybrid risks, develop analytical and forecasting tools, strengthen cyber defences and critical infrastructure, and strategically apply coordination mechanisms between government and society to ensure national resilience [54].

To enhance the capacity of EU Member States to counter hybrid threats and ensure the resilience of national security systems, the "EU Strategic Compass for Security and Defence" [51] is utilised to enhance the ability of EU Member States to counter hybrid threats and ensure the resilience of national security systems; it sets out clear priorities for crisis prevention, strengthening defence capabilities, and developing resilient institutions and integrated mechanisms for responding to threats, combining military, economic, information and cyber tools.

The EU Strategic Compass emphasises the need for a comprehensive approach to countering hybrid threats, which includes:

– the development of effective early-warning systems;

– the establishment of flexible and responsive coordination mechanisms between Member States;

– the strengthening of cyber security, critical infrastructure and communication channels;

– the training and preparation of personnel to respond to crisis and hybrid situations.

The EU Strategic Compass serves as a tool for building collective resilience to contemporary threats, strengthening states' defence capabilities and supporting democratic institutions in a world where hybrid risks are becoming one of the most significant challenges to security and economic stability. An important aspect of implementing the Compass is enhancing the resilience of economic and social systems,

as economic stability is a critical component of national security. The EU Strategic Compass calls on Member States to integrate the assessment of hybrid risks into their national security strategies, as well as to ensure joint training and the exchange of knowledge on identifying, neutralising and minimising the consequences of hybrid attacks [51].

Guiding principles for the provision of EU support to build economic resilience in partner states have been set out in official documents, and it has been noted that building resilience and defining the relevant political, economic, environmental and social priorities are matters of national responsibility [56]. For Ukraine, the implementation of similar approaches and integration into the relevant European mechanisms is becoming particularly relevant in the context of protecting the national economy and ensuring the continuity of state functions in times of crisis (Fig. 3.12).

In this context, it is important to adopt European practices for identifying threats to economic security, which are based on a systematic and multi-level approach and combine strategic forecasting, continuous risk monitoring and inter-institutional coordination [58]. The starting point is an understanding of economic security as a complex concept, vulnerable to external and internal shocks arising from geopolitical instability, technological shifts, climate change and structural imbalances in development.

The practice of early risk detection is implemented through regular strategic reviews and analytical reports by European institutions. The European Commission, the European External Action Service, the European Central Bank and specialised EU agencies assess vulnerabilities in the internal market, the financial system, supply chains and critical infrastructure [57]. Particular attention is paid to dependence on imports of strategic resources, the concentration of production in third countries and the risks of economic coercion.

European practices for identifying threats to economic security and building an ecosystem of economic resilience are characterised by their comprehensive nature, their preventative focus and their orientation towards long-term sustainability. Their application provides a methodological basis for adapting similar approaches in Ukraine, taking into account military challenges and the course towards deeper integration with the European Union.

Assessing the impact of threats on the resilience of the European security space is regarded as an integral part of formulating effective economic and general security policies. In the EU's current approach, resilience is not merely the ability to withstand crises, but also the capacity of economic, institutional and social systems to adapt to prolonged destabilising influences, to recover from shocks and to maintain functional integrity in the long term [52].

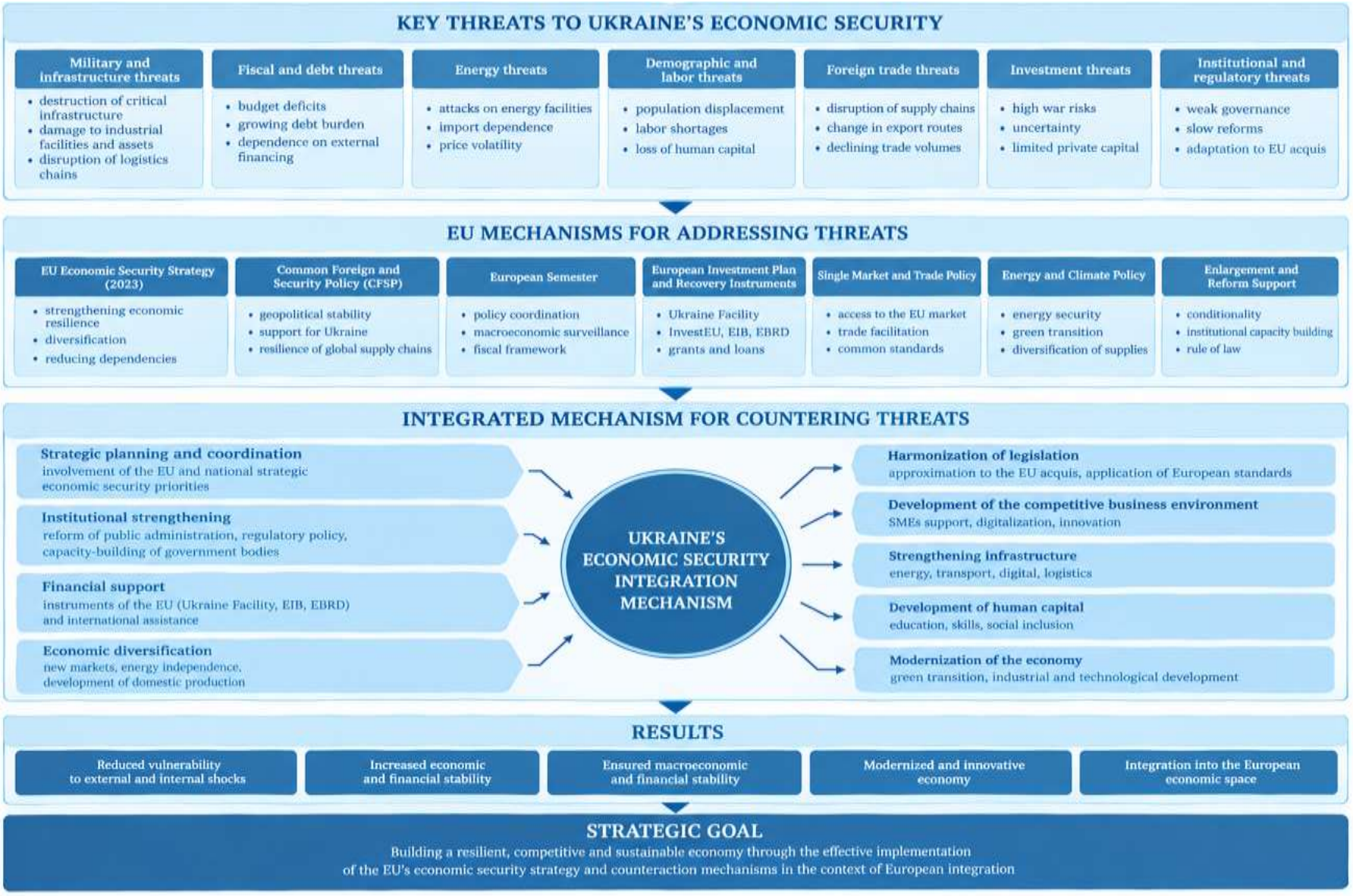


Fig. 3.12. The EU's economic sustainability ecosystem for Ukraine

At present, the EU's economic resilience ecosystem is based on the ability of Member States and the EU as a whole to withstand a wide range of threats, whilst upholding shared democratic values. The EU's strategic approach to economic resilience is underpinned by the following principles [57]:

1) investing in resilience is more cost-effective than reacting to crises after the event, as the increasing frequency and intensity of disasters and humanitarian crises mean that the severity of their consequences for developing countries poses the main threat to long-term development;

2) it is advisable to focus primarily on areas of vulnerability and to address the root causes of crises (particularly chronic poverty), rather than the consequences of the problems.

This requires the development of appropriate policies covering several components: risk assessment; taking measures to reduce, prevent and mitigate risks, and ensure preparedness; strengthening capacity for rapid crisis response and recovery.

A key feature of European practice in ensuring economic resilience is the use of scenario modelling and stress testing to identify the potential consequences of various types of threats. These tools are used to assess the possible outcomes of protracted armed conflicts, large-scale cyber-attacks, disruptions to the supply of energy resources and critical raw materials, as well as financial crises [60]. In doing so, the focus is not only on the likelihood of a particular threat occurring, but also on the scale of its potential impact on economic stability, the functioning of critical sectors, and social cohesion within EU Member States.

A key aspect of such an assessment is identifying the interdependence and cumulative nature of risks. Economic disruptions may be accompanied simultaneously by destabilising factors relating to security, technology and information, thereby amplifying the cumulative effect of individual threats. European approaches therefore involve analysing not only the direct consequences but also the cross-sectoral and cross-border effects arising from the spread of crisis phenomena across interconnected systems. This creates opportunities to identify the most vulnerable elements of the European security landscape and to determine ways of strengthening them [57].

The organisational prerequisite for such an assessment is cooperation between EU institutions in particular the European Commission, the European External Action Service and the Council of the European Union as well as relevant agencies and the competent authorities of the Member States. Coordination of their activities ensures the harmonisation of information and analytical approaches, facilitates a more comprehensive assessment of risk levels and creates the conditions for the development of coordinated response mechanisms.

The results of threat impact assessments form the information and analytical basis for the strategic management of the EU's economic security. On this basis,

priorities are set for reducing critical dependencies, diversifying supply sources, developing domestic production capacities, strengthening strategic autonomy and enhancing the economy's resilience to external shocks. For Ukraine, given its deepening integration into the European economic and security space, the adaptation of relevant methodological and institutional approaches is an important prerequisite for aligning national policy with European Union practices.

The development of mechanisms to prevent and neutralise threats to the economic security of EU Member States has taken place gradually, driven by changes in the global economic environment, intensifying geo-economic competition, the accumulation of systemic crisis risks and the escalation of security challenges. In the current climate, the European system of economic resilience relies on a combination of regulatory, institutional, financial and organisational-economic instruments [55]. Their purpose is not only to minimise the consequences of threats that have already materialised, but also to build the capacity to identify and mitigate potential sources of destabilisation at an early stage.

One of the priority areas of such a policy is the reduction of critical external dependencies in strategically important sectors. EU Member States and institutions are diversifying their sources of supply for energy resources, critical raw materials, technologies and intermediate components, whilst supporting the development of production capacities within the European Union and deepening cooperation with reliable international partners. In this context, diversification is viewed as a means of reducing risk concentration and enhancing the economy's resilience to disruptions in international supply chains [59].

A separate set of measures relates to the regulation of economic interaction with third countries. The EU is strengthening mechanisms for screening foreign investment in strategically sensitive sectors, improving controls on the export of dual-use goods and technologies, and applying restrictive measures in cases where economic ties pose security risks. These instruments are designed to prevent external actors from gaining access to critical infrastructure, technological capabilities, strategic assets or resources, the use of which could pose additional threats to the EU's economic and security resilience.

At the same time, an important component of preventive policy is the development of mechanisms for strategic forecasting, monitoring and early detection of risks. The use of analytical tools, digital monitoring systems and mechanisms for inter-institutional information exchange enhances the capacity to identify potential threats in a timely manner and assess their possible consequences. This makes it possible to enhance the preparedness of state institutions to deal with crisis scenarios, reduce the time between the detection of a risk and the response to it, and, consequently, minimise potential losses to the economy. In the current context, the key

conditions for ensuring economic resilience include sustainable development, economic stability, good governance and the protection of human rights.

Within the European ecosystem of economic resilience, considerable attention is paid to strengthening the state's institutional capacity and building its readiness to respond to external risks [58]. This approach encompasses the creation of the necessary resource and organisational reserves, the improvement of coordination between state authorities, and the alignment of national measures with mechanisms implemented at European Union level. At the same time, the private sector is becoming increasingly involved in economic security measures, which promotes the sharing of responsibility between state and non-state actors and strengthens the economy's overall capacity to counter external destabilising influences.

Financial support constitutes another avenue for countering external shocks. In the practice of EU Member States, various forms of support are employed, including stabilisation instruments, state aid programmes for enterprises, preferential and anti-crisis lending, as well as risk insurance mechanisms [57]. Their use makes it possible to limit the negative impact of crises on the financial position of businesses and households, to sustain employment and to ensure the continued functioning of sectors critical to the economy.

The experience of EU countries demonstrates the dynamic nature of the system for preventing and neutralising threats to economic security. Its effectiveness depends to a large extent on the ability to review existing instruments in a timely manner, adapt response mechanisms and supplement them in line with changes in the global economic and security environment. For Ukraine, which is simultaneously confronting large-scale external challenges and deepening its integration into the European economic and security space, the application of relevant European practices could become one of the avenues for strengthening national economic resilience and developing a system of preventive protection against external threats.

For Ukraine, European integration provides a fundamentally important mechanism for countering threats to the state's economic security, as deeper access to the European market, financial support, institutional convergence, participation in European programmes, harmonisation of the regulatory environment and the attraction of European capital can create additional sources of economic resilience.

A prime example in this regard is the Ukraine Facility [61], which combines financial support for Ukraine with the implementation of structural reforms and investment measures. The European Commission describes the Ukraine Facility precisely as an instrument that simultaneously supports Ukraine's financial needs, its recovery and modernisation, and the advancement of the reforms necessary for EU accession. Key areas of this programme include macro-financial stability, public administration reform, sound management of public finances, the fight against corruption, attracting investment, and aligning Ukrainian legislation with EU law.

Therefore, European integration reforms must be viewed not as a process external to economic security, but as one of the mechanisms for its long-term strengthening. Ukraine's recovery and its European integration should be viewed as interlinked processes. The scale of reconstruction needs means that rebuilding is not merely a matter of compensating for war-related losses, but a structural project to transform the economy.

Meeting the criteria and requirements for EU accession creates an institutional environment capable of mitigating some of the systemic internal threats to economic security. The European Commission explicitly links the Ukraine Plan to the recovery and modernisation of the economy and to bringing Ukraine closer to EU law. At the same time, insufficient institutional capacity, delays in reforms or weak mechanisms for monitoring the use of public resources may become a factor in economic vulnerability. EU documents explicitly emphasise the need to strengthen Ukraine's institutional and administrative capacity as part of the process of aligning with EU legislation.

Thus, in the long term, Ukraine's economic security must be shaped at the intersection of three interrelated components: military resilience, macroeconomic and financial stability, and the institutional and structural reorganisation of the economy. It is the synchronisation of these components that will determine Ukraine's ability not only to withstand current threats, but also to transition from a regime of economic survival under wartime conditions to a model of sustainable development within the European economic area.

Reference:

1. Chimits, F., McCaffrey, C., Mejino Lopez, J., Poitiers, N., Vicard, V. & Wibaux, P. (2024). European Economic Security: Current Practices and Further Development, INTA committee study, 2 May.

2. Vicard, V. & Wibaux, P. (2023). EU Strategic Dependencies: A Long View. CEPII Policy Brief no. 2023-41.

3. Maslii, O., Buriak, A., Chaikina, A., & Cherviak, A. (2025). Improving conceptual approaches to ensuring state economic security under conditions of digitalization. Eastern-European Journal of Enterprise Technologies, 1(13 (133), 35–45. https://doi.org/10.15587/1729-4061.2025.319256

4. European Commission. (2023). Joint Communication to the European Parliament, the European Council and the Council on «European Economic Security Strategy». JOIN (2023) 20 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023JC0020

5. European Commission. (2024a). Advancing European economic security: An introduction to five new initiatives. COM (2024) 22 final. https://commission.europa.eu/document/download/8b5910fe-10ea-4645-8b14-162ff72ea049_en?filename=Communication+on+European+economic+security.pdf&utm_source=chatgpt.com

6. European Commission. (2025a). Strengthening EU economic security. JOIN (2025) 977 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex: 52025JC0977

7. Council of the European Union. (2026a). European economic security. https://www.consilium.europa.eu/en/policies/european-economic-security/

8. Council of the European Union. (2026b). Competitiveness compass. https://www.consilium.europa.eu/en/policies/competitiveness-compass/#security

9. European Commission. (2025b). The EU Startup and Scaleup Strategy: Choose Europe to start and scale. COM (2025) 270 final. https://data.consilium.europa.eu/doc/document/ST-9607-2025-INIT/en/pdf

10. Council of the European Union. (2024). Council Recommendation on enhancing research security. ST 9097/1/24 REV 1. https://data.consilium.europa.eu/doc/document/ST-9097-2024-REV-1/en/pdf

11. Council of the European Union. (2025). European Research Area. https://www.consilium.europa.eu/en/policies/european-research-area/

12. European Commission. (2025b). Proposal for a Council Recommendation on the European Research Area Policy Agenda 2025–2027. COM (2025) 62 final. https://european-research-area.ec.europa.eu/sites/default/files/documents/2025-02/COM_2025_62_F1_PROPOSAL_FOR_A_RECOMMENDATION_EN_V5_P1_3951028.PDF

13. European Commission. (2025c). A European strategy on research and technology infrastructures. COM (2025) 497 final/2. https://data.consilium.europa.eu/doc/document/ST-12895-2025-REV-1/en/pdf

14. European Investment Bank. (2026). Investment Report 2025/26: Capitalising on Europe's strengths. European Investment Bank. DOI: 10.2867/0714109. https://www.eib.org/files/publications/20250379-030326-investment-report-2025-en.pdf

15. United Nations Statistics Division. (2025). UN Comtrade Database. https://comtradeplus.un.org/

16. European Commission (2021). Strategic dependencies and capacities. Commission Staff Working Document, SWD (2021) 352.

17. Vicard, V. & Wibaux, P. (2023). EU Strategic Dependencies: A Long View. CEPII Policy Brief no. 2023-41.

18. Eurostat. (2026). International trade in goods: Database. European Commission. https://ec.europa.eu/eurostat/web/international-trade-in-goods/database

19. European Commission. (2024b). Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council. COM (2024) 23 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX:52024PC0023&utm_source=chatgpt.com

20. European Commission. (2024c). White Paper on Outbound Investments. COM (2024) 24 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A52024DC0024&utm_source=chatgpt.com

21. European Commission. (2024d). White Paper on Export Controls. COM (2024) 25 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX:52024DC0025&utm_source=chatgpt.com

22. European Commission. (2024e). White Paper on options for enhancing support for research and development involving technologies with dual-use potential. COM (2024) 27 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52024DC0027&utm_source=chatgpt.com

23. Buriak, A., & Maslii, O. (2025). European Approaches to Enhancing the State's Economic Security through the Development of Cyber Resilience. Kyiv Economic Scientific Journal, (11), 53-62. https://doi.org/10.32782/2786-765X/2025-11-7

24. Onyshchenko, S., Maslii, O., & Hlushko, A. (2025). Digital and economic security of the state under global threats. Lecture Notes in Networks and Systems, 1338, 580–602. https://doi.org/10.1007/978-3-031-89296-7_29

25. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity and improvement of the information security system. Journal of the Balkan Tribological Association, 29(5), 818–835. https://www.scopus.com/record/display.uri? eid=2-s2.0-85181654278&origin=recordpage

26. Onyshchenko, S., Hlushko, A., Maslii, O., & Chumak, O. (2024). Digital transformation of the national economy in the context of information environment development in Ukraine. Transformations of national economies under conditions of instability, 169–197.

27. European Commission. (2025c). RESourceEU Action Plan: Accelerating our critical raw materials strategy to adapt to a new reality. COM(2025) 945 final. https://single-market-economy.ec.europa.eu/document/download/01c448d6-dc93-40d7-9afe-4c2af448d00c_en

28. Maslii, O. (2025). Concepts of protecting national economic interests in the global information space. Economics and Management, 3(105), 33–39. https://doi.org/10.32782/2312-7872.3.2025.4

29. Yakymenko, Yu., & Yurchyshyn, V. (2024). Geopolitical challenges and geoeconomic shifts. Razumkov Center. https://razumkov.org.ua/images/2024/07/ 12/2024-PAKT-11-2.pdf

30. Maslii, O.A., Kivshyk, O.P., & Kotelevets, M.M. (2023). Threats to the Economic Security of the State under Global Transformations. Economic space, 183, 25–29. https://doi.org/10.32782/2224-6282/183-4

31. Pugach, O. (2015). Modelling the threats to the economic security system of the national economy in terms of their timely detection and prediction. Economy and Region, 3(52), 103–109. https://reposit.nupp.edu.ua/item/2842

32. Zhalilo, Ya. A. (Ed.). (2024). Economic security of Ukraine in the context of a protracted war. Kyiv : NISS. https://doi.org/10.53679/NISSanalytrep.2024.08

33. World Economic Forum. (2026). The Global Risks Report 2026. World Economic Forum. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf

34. Maslii, O., & Galushka, R. (2025). Hierarchical Analysis of Risks and Threats to Ukraine's Economic Security under Martial Law. Economic space, 198, 67–75. https://doi.org/10.30838/EP.198.69-75

35. Baranovskyi, O. I. (2014). Philosophy of security. Kyiv: UBS NBU. 830 p.

36. World Economic Forum. (2025). Chief Economists Outlook. https://reports.weforum.org/docs/WEF_Chief_Economists_Outlook_September_2025.pdf

37. Dunn Cavelty, M., Grgić, G., Mockli, D., Perović, J., Schepers, N., & Singh, M. (2025). Strategic Trends 2025: Key Developments in Global Affairs. ETH Zurich, Centre for Security Studies. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ST2025-01-DM.pdf

38. Del Cerro, C.C. (2024). The power of social networks and social media's filter bubble in shaping polarisation: An agent-based model. Appl. Netw. Sci., 9, 69.

39. Federal Reserve Bank of St. Louis. (2025). Real Residential Property Prices for Advanced Economies (aggregate). Data from the Bank for International Settlements (BIS). https://fred.stlouisfed.org/series/Q5RR628BIS

40. Inderwildi, O. (2025, April 14). The Quantum Computing Revolution: From Technological Opportunity to Geopolitical Power Shift, (Part 2). The Geopolitical Economist. Medium. https://medium.com/the-geopolitical-economist/the-quantumcomputing-revolution-geopolitics-economics-c2380e0167ee

41. Tran, Duc Le, Phuc, Hao Do, Truong, Duy Dinh, & Van Dai, Pham. (2025). Are Enterprises Ready for Quantum-Safe Cybersecurity? arXiv. https://arxiv.org/pdf/2509.01731

42. Auer, R., Dupont, A., Gambacorta, L., et al. (2024). Quantum computing and the financial system: opportunities and risks (BIS Papers No 149). Bank for International Settlements (BIS). https://www.bis.org/publ/bppdf/bispap149.pdf.

43. Onyshchenko S., Maslii O., Hlushko A., Huba L., Barabash V. (2025). Threats and dangers to economic security of Ukraine in the terms of war. Rivista Di Studi Sulla Sostenibilità – Review of Studies on Sustainability, 10 (2). https://doi.org/10.3280/riss2025oa19683

44. International Monetary Fund. Ukraine: 2026 Article IV Consultation and First Review of the Extended Arrangement Under the Extended Fund Facility. IMF Staff Country Report, 2026. https://www.elibrary.imf.org/view/journals/002/2026/ 188/article-A001-en.xml

45. OECD. (2025). OECD Economic Surveys: Ukraine 2025. Paris: OECD Publishing. https://www.oecd.org/en/publications/oecd-economic-surveys-ukraine-2025_940cee85-en.html

46. World Bank. (2026). Updated Ukraine Recovery and Reconstruction Needs Assessment (RDNA5). https://www.worldbank.org/uk/news/press-release/2026/02/ 23/updated-ukraine-recovery-and-reconstruction-needs-assessment-released

47. United Nations Office of Counter-Terrorism. (2022). The Protection of Critical Infrastructure Against Terrorist Attacks, 2022 Update. https://www.un.org/counterterrorism/sites/default/files/2225521_compendium_of_good_practice_web.pdf

48. European Commission. (2025d). Progress towards Meeting the Economic Criteria for EU Accession: 2025 European Commission Assessments. Institutional Paper 329. Brussels, 2025. https://economy-finance.ec.europa.eu/publications/ progress-towards-meeting-economic-criteria-eu-accession-2025-european-commission-assessments_en

49. European Commission. (2026c). EU-Ukraine Solidarity Lanes. https://commission.europa.eu/topics/eu-solidarity-ukraine/eu-assistance-ukraine/eu-ukraine-solidarity-lanes_en

50. European Commission (2025e). Ukraine Report 2025. Brussels. https://enlargement.ec.europa.eu/ukraine-report-2025_en

51. A Strategic Compass for Security and Defence. European External Action Service. URL: https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en

52. Reznikova, O. O. (2022). National resilience in a changing security environment. Kyiv: NISS. 456 p. https://doi.org/10.53679/NISS-book.2022.01

53. Jungwirth, R., Smith, H., et al. (April 2023). Hybrid Threats: A Comprehensive Resilience Ecosystem. Joint Research Centre, European Commission, and the European Centre of Excellence for Countering Hybrid Threats. 123 p. https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_ resilience_ecosystem.pdf

54. Maslii, O. A., Maksymenko, A. P. (2023). Risks and threats to the economic security of Ukraine in the digital sphere in the conditions of war. Market economy: modern management theory and practice, 21, 3(52), 179–199. https://doi.org/10.18524/2413-9998.2022.3(52).275802

55. The European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/aboutus/

56. Resilience Dashboards. Update Spring 2023. European Commission. 53 p. https://jeodpp.jrc.ec.europa.eu/ftp/jrc-opendata/RESILIENCEDASHBOARDS/Spring2023Update/Dashboard_SpringUpdate_2023.pdf

57. Heyets, V.M., Burlai, T.V., & Blyzniuk, V.V. (2023). Social Resilience of the National Economy Through the Prism of the Experience of the European Union and Ukraine. Economic Theory, 3, 5–43. https://doi.org/10.15407/etet2023.03

58. Varnaliy, Z., Onishchenko, S., Masliy, A. (2016). Threat prevention mechanisms of Ukraine's economic security. Economic Annals-XXI, 159(5-6), 20-24.

59. Danylyshyn B.M., Onyshchenko S.V., Maslii O.A. (2019) Socio-economic security: modern approach to ensuring the socio-economic development of the region. Economy and Region, 4(75), 6–13.

60. Masliy, O.A., Kudinova, A.O., Buryak, A.A., Yanko, A.S., Bilko, S.S. (2025). Determinants of the economic security of the state in the paradigm of digital development: monograph. Ivano-Frankivsk: NAIR, 324 p.

61. European Commission. (2026d). Ukraine Facility. https://enlargement.ec.europa.eu/funding-technical-assistance/ukraine-facility_en

CHAPTER 4

INFORMATION AND CYBERSECURITY OF UKRAINE IN THE ARCHITECTURE OF EUROPEAN DIGITAL RESILIENCE



4.1. Institutional framework for ensuring information security and digital resilience of the European Union

The digitalization of socio-economic processes and the rapid growth of the role of information technologies have led to a transformation of ideas about security in modern international relations. Information security is increasingly viewed not as an auxiliary technical element, but as a key component of the strategic autonomy of states and supranational entities [1]. For the European Union, which functions as a complex political and economic system with a high level of interdependence, the protection of the information space is of particular importance. In this context, the EU Global Strategy "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy" [2] became a conceptual document that laid the foundations for the integration of information security into the system of strategic goals of the Union.

Presented in June 2016, the EU Global Strategy (EUGS) was formed in the context of increasing instability in the international environment, the spread of hybrid threats, cyberattacks, external information influence and systemic disinformation. The document demonstrated a departure from a narrow interpretation of security and a transition to a comprehensive approach that combines foreign policy, security, economic and social dimensions. One of the key categories of the EUGS was "resilience", which is associated with the ability of states, societies and institutions to withstand internal and external shocks, adapt to them and maintain functional capacity [2]. Information security in the EUGS was not yet distinguished as an independent policy direction in its modern understanding, however, its basic elements were integrated due to the need to strengthen democratic institutions, social resilience, countering hybrid threats, developing cybersecurity and strategic communications. That is why it is advisable to consider the EUGS not as a normative source of information security regulation, but as a conceptual prerequisite for the further formation of the relevant EU policy.

The understanding of security through the category of resilience, enshrined in the Global Strategy, has gradually been concretized in a complex of strategic, normative, regulatory and organizational mechanisms. As the digital transformation deepens, the emphasis has shifted from protecting information and information and communication systems as separate objects to ensuring the security of the information environment, democratic processes, digital infrastructure, media space and public trust.

While the early stages of the development of European information policy focused on ensuring access to information, protecting personal data, developing the information society and ensuring the safe functioning of information and communication networks, the current stage is characterized by a significant expansion of the content and areas of information security policy. These include countering disinformation, foreign information manipulation and interference, protecting democratic processes, ensuring the transparency of digital platforms, preserving media pluralism, identifying artificially generated content, protecting information systems and increasing the resilience of society to destructive information influence [3].

Ensuring information security is advisable to consider precisely from the standpoint of an institutional approach, since the effectiveness of the relevant policy is determined not only by the availability of technological means of protection, but also by the formation of a system of formal rules, regulatory mechanisms and organizations responsible for their implementation [4]. Studies confirm that the systematic nature of information security is ensured by a combination of regulatory, organizational and technological mechanisms, and European experience constitutes an important institutional basis for the development of national information and cybersecurity systems [3–5].

Methodologically, it is important to consider that the law of the European Union has not formed a single regulatory act that would comprehensively regulate information security in the broad interpretation of this category. There is also no single supranational body endowed with the full range of competences for the protection of the information space. Instead, a system of distributed powers has been formed, within which various regulatory and legal acts and institutions provide separate but interrelated areas: protection of information and personal data; countering disinformation and FIMI; security of digital platforms and the media environment; cybersecurity of networks and information systems; protection of democratic and electoral processes; transparency of political communication; digital and operational resilience.

Based on this, it is proposed to interpret the institutional provision of information security of the European Union as a system of interconnected formal rules, strategic and regulatory instruments, supranational and national institutions, specialized agencies, regulatory bodies, coordination networks and expert and analytical structures, the interaction of which is aimed at protecting information and the information environment, minimizing information and cyber risks, ensuring the stability of democratic processes and the safe functioning of the EU digital environment.

The author's structuring of institutional support for information security is based on the identification of two interrelated components:

1) institutional and legal support, which includes strategic documents, legal and regulatory acts that define the goals, principles, rules, rights, obligations and mechanisms for ensuring information security;

2) institutional and organizational support, represented by EU political and regulatory institutions, specialized agencies, law enforcement structures, coordination networks, information and analytical platforms, and expert and research structures that ensure the implementation, coordination, monitoring, and development of relevant policies.

The relationship between these components and their subject content is systematized in Figure 4.1.

The institutional and legal component of the system under study was formed gradually and reflects the evolution of the understanding of information threats itself. Its specificity lies in the combination of acts of different legal nature: regulations and directives, which create binding rules for Member States and economic entities; strategies and communications of the European Commission, which define policy priorities; as well as co-regulatory mechanisms, which include codes of conduct of digital platforms.

As can be seen from Figure 4.1, it is advisable to structure institutional and legal support not according to the formal and legal basis of dividing acts into regulations, directives and decisions, but according to the main areas of their regulatory impact.

This approach makes it possible to trace which segments of information security are covered by the EU legal field, as well as to establish their relationship with the relevant institutions and implementation mechanisms. Within the framework of the proposed systematization, four blocks are distinguished: strategic documents; protection of information and personal data; protection of the information and media environment; cybersecurity and digital resilience.

The first block of institutional and legal support is formed by strategic documents that define the general directions of development of European security, digital and information policy. Their function is not to establish directly binding rules of conduct, but to define the goals, priorities and directions of further regulatory and legal regulation.

Following the EUGS 2016, an important milestone was the Communication Tackling online disinformation: a European Approach 2018, which identified disinformation as a systemic challenge to democratic processes, the free formation of political will and public trust [6]. The subsequent Action Plan against Disinformation established four policy areas: strengthening the capacity of EU institutions to detect and analyse disinformation; ensuring a coordinated response; mobilising the private sector; and increasing public awareness and resilience [7]. The EU Security Union Strategy 2020 further consolidated the understanding of the interconnectedness of the physical and digital environments, cyber threats, hybrid influences and the protection of critical societal functions [8]. The European Democracy Action Plan 2020, in turn, integrated countering disinformation into a broader mechanism for protecting democracy, combining it with ensuring fair elections, freedom and pluralism of the media [9].



Fig. 4.1. Structural and logical diagram of the institutional support of information security of the European Union

In the same year, 2020, The EU's Cybersecurity Strategy for the Digital Decade identified cybersecurity as a necessary prerequisite for digital transformation, the functioning of the economy and democratic institutions [10]. The next steps were the 2030 Digital Compass of 2021 [11], the Strategic Compass for Security and Defence of 2022 [12] and Decision (EU) 2022/2481, which established the Digital Decade Policy Programme 2030 [13]. Taken together, these documents have established security, resilience, digital capabilities and the protection of fundamental rights as interrelated characteristics of the European digital transformation.

The security context was expanded in the European Economic Security Strategy 2023, where cyberattacks, foreign interference and disinformation are explicitly considered as sources of risk, alongside technological dependence and threats to critical infrastructure [14]. Further development of this direction is reflected in the European Democracy Shield 2025, which envisages strengthening the protection of democratic processes, information integrity and the EU's ability to counter external information interference [15].

Therefore, the development of the strategic level demonstrates a gradual transition from a fragmented response to individual types of information threats to the inclusion of information environment security in the system of democratic, economic, technological and digital resilience of the EU.

The second block of institutional and legal support is formed by the system of information and personal data protection. Its fundamental act is Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR), which established uniform principles and requirements for the processing of personal data, the rights of data subjects, the liability of controllers and processors and the activities of independent supervisory authorities [16]. It is complemented by Directive (EU) 2016/680, which regulates the processing of personal data by competent authorities in the field of prevention and investigation of criminal offences [17], and Regulation (EU) 2018/1725, which defines the rules for the protection of personal data in the activities of the institutions, bodies, offices and agencies of the European Union [18]. Thus, data protection acquires a systemic nature and covers both the private and public sectors of the Member States and the supranational level of EU governance.

The inclusion of this block in the institutional information security system is fundamentally important, as violations of the confidentiality, integrity, or legality of information processing create not only individual risks for data subjects, but also broader risks to trust in digital services and institutions.

The third block is the most dynamic and reflects the EU's transition from predominantly voluntary mechanisms to counter disinformation to a combination of legislative regulation and mechanisms for co-regulation of the activities of digital platforms, media entities and other participants in information relations. A qualitatively

new stage is associated with Regulation (EU) 2022/2065 – Digital Services Act (DSA) [19]. Its significance for information security lies in establishing obligations for very large online platforms and search engines to assess and minimize systemic risks that may have a negative impact on fundamental rights, civil discourse, electoral processes and public security.

Thus, in the European model, the very logic of responsibility of digital intermediaries is changing: they are no longer considered exclusively as neutral channels for the dissemination of information, but are involved in the systemic risk management of the digital information environment.

An important co-regulatory instrument was the Strengthened Code of Practice on Disinformation 2022, which included commitments to demonetize disinformation resources, transparency in advertising, countering manipulative behavior, cooperating with fact-checkers, and ensuring access to data for researchers [20]. In February 2025, the European Commission and the European Board for Digital Services approved the integration of its commitments into the DSA regulatory framework as the Code of Conduct on Disinformation, which strengthened the connection of co-regulatory mechanisms with the formal legal regime of digital services [21].

A separate direction is formed by Regulation (EU) 2024/1083 – European Media Freedom Act (EMFA) [22]. Its institutional significance lies in the formation of a pan-European framework for the protection of editorial independence, transparency of media ownership, media pluralism and the proper functioning of the internal market for media services. An important result of EMFA was the creation of the European Board for Media Services, which replaced the European Regulators Group for Audiovisual Media Services from 2025.

The protection of the media environment is also related to Directive (EU) 2018/1808, which modernised the Audiovisual Media Services Directive in line with changes in the digital media market and extended certain requirements to video platforms [23]. Regulation (EU) 2024/900 on the transparency and targeting of political advertising [24] introduced common rules for the identification of political advertising, the transparency of its financing and the use of targeting technologies. The main part of the provisions of the Regulation has been applicable since 10 October 2025, which is particularly important for limiting opaque microtargeting and the manipulative use of personal data in political communication.

Of particular importance in the context of the spread of generative technologies is Regulation (EU) 2024/1689 – Artificial Intelligence Act [25]. Article 50 of the Act establishes special transparency requirements for certain content created or manipulated with the help of artificial intelligence, including deepfake content. Therefore, the subject of institutional protection is not only the channel of information

dissemination, but also the technological method of its creation and the possibility of identifying its artificial origin.

Together, the DSA, EMFA, political advertising rules, the AI Act, the AVMSD and mechanisms to counter disinformation form a set of regulatory instruments to protect the information and media environment. Its specific feature is the need to simultaneously counter manipulative influences and preserve freedom of expression, media pluralism and other fundamental rights [26].

Another area of legal regulation is related to the technological security of the information environment. Its basic acts include Regulation (EU) 2019/881 – Cybersecurity Act [27] and Directive (EU) 2022/2555 – NIS2 Directive [28]. The Cybersecurity Act established a permanent mandate for ENISA and created a European framework for cybersecurity certification of information and communication technologies, while NIS2 significantly expanded the sectoral coverage, requirements for cyber risk management, incident reporting, oversight and liability. An important addition is Directive (EU) 2022/2557 – Critical Entities Resilience Directive (CER), aimed at increasing the resilience of critical entities to a range of natural and anthropogenic risks [29]. The joint operation of NIS2 and CER reflects the interrelationship of the cyber and physical dimensions of the resilience of critical systems.

A special place is occupied by Regulation (EU, Euratom) 2023/2841, which establishes measures to achieve a high common level of cybersecurity in the EU institutions, bodies, offices and agencies, establishes the role of CERT-EU and creates the Interinstitutional Cybersecurity Board (IICB) [30]. Further expansion of the legal framework was provided by Regulation (EU) 2024/2847 – Cyber Resilience Act, which established horizontal cybersecurity requirements for products with digital elements throughout their life cycle [31]. In this way, responsibility for digital resilience is transferred to the stages of design, production, implementation and support of digital products.

Regulation (EU) 2025/38 – Cyber Solidarity Act, adopted on 19 December 2024 and published on 15 January 2025, develops not only the preventive but also the collective component of European cyber resilience, creating mechanisms for joint detection, preparation and response to large-scale cyber threats and incidents [32]. For the financial sector, the relevant direction is specified in Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA), which establishes requirements for ICT risk management, operational resilience testing, incident management and risks of third-party ICT suppliers [33].

Thus, the fourth regulatory block provides the legal and organizational prerequisites for the technological security of information and information systems. The protection of the information environment directly depends on the stability of

networks, digital products, critical entities, information systems and ICT infrastructure of EU institutions. This is where the objective relationship between information security and cybersecurity is revealed [1, 3].

If the institutional and legal component determines the formal rules of the functioning of the information environment, then the institutional and organizational component ensures their development, implementation, coordination and control. As systematized in the right part of Figure 4.1, it is advisable to structure it according to the functions and competencies of the subjects, highlighting political and regulatory institutions; analytical and information platforms and foreign policy structures; agencies in the field of cybersecurity and digital infrastructure; law enforcement structures; regulatory and coordination bodies in the field of digital services, media and data protection; coordination response networks; expert, analytical and research structures.

The basic policy-regulatory level is formed by the European Commission, the European Parliament, the Council of the European Union and the European Council. The leading role in the formation and implementation of regulatory policy belongs to the European Commission. It initiates legislative acts, determines the strategic directions of digital and information policy, monitors the application of EU legislation and exercises special supervisory powers provided for in individual regulatory acts. In its structure, the Directorate-General for Communications Networks, Content and Technology (DG CONNECT) is of particular importance, its activities covering digital services, online platforms, media policy, artificial intelligence, cybersecurity and countering disinformation.

A separate area of analytical and foreign policy activity in the field of information security is associated with the European External Action Service (EEAS). Since 2015, the East StratCom Task Force, established within its structure, has been developing capabilities to detect and analyze disinformation campaigns, and the EUvsDisinfo platform provides for their systematic monitoring and public coverage. After the Action Plan against Disinformation, the Rapid Alert System was introduced, which ensures the exchange of information between EU institutions and member states on disinformation campaigns [7, 34].

The current EEAS policy increasingly uses the concept of Foreign Information Manipulation and Interference (FIMI), which allows for a shift in analytical focus from verifying the veracity of a single message to a systematic study of the actor, their behavior, coordination, distribution channels, and strategic intent [34]. This is particularly important for distinguishing between ordinary disinformation and organized external information interference.

The main EU specialized agency in the field of cybersecurity is the European Union Agency for Cybersecurity (ENISA). Its mandate, according to the Cybersecurity

Act, includes support to the Member States and the Union institutions, development of an expert base, facilitation of the implementation of legislation, certification, assessment of cyber risks and development of a common cybersecurity culture [27]. At the same time, in the proposed model, ENISA is considered not as a universal information security authority, but as a specialized institution, responsible primarily for its technological and cyber segment.

The same block includes CERT-EU, which provides cybersecurity support to EU institutions, bodies, offices and agencies in accordance with Regulation (EU, Euratom) 2023/2841 [30], and eu-LISA, the agency responsible for the operational management of large-scale IT systems in the area of freedom, security and justice.

The law enforcement segment is represented primarily by Europol and its European Cybercrime Centre (EC3). Its functional purpose is to support Member States in investigating complex cross-border cybercrime, provide analytical support for operations and coordinate law enforcement cooperation [35]. Thus, EC3 complements preventive and regulatory instruments with mechanisms to counter criminal manifestations in the digital environment.

An independent institutional unit is formed by regulatory coordination bodies in the field of digital services, media and data protection. The European Board for Digital Services, established under the DSA, brings together Digital Services Coordinators of the Member States and promotes the consistent application of the DSA throughout the Union [36]. The European Board for Media Services, established under the EMFA, coordinates the activities of national media regulators and promotes the consistent application of media legislation [22].

In the area of personal data protection, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) are of central importance. The EDPB ensures the consistent application of the GDPR at the level of the Member States, while the EDPS is an independent supervisory authority for the processing of personal data by the EU institutions, bodies, offices and agencies [18, 37]. This division of competences ensures the interaction of the national and supranational levels of data protection.

The cybersecurity coordination mechanism is represented by the NIS Cooperation Group, the CSIRTs Network and the EU-CyCLONe. The NIS Cooperation Group ensures strategic cooperation and information exchange between Member States, the CSIRTs Network – operational and technical interaction of incident response teams, while the EU-CyCLONe is focused on coordinating the management of large-scale cyber incidents and crises [28]. At the level of the EU's own institutions, the relevant coordination mechanism is complemented by the Interinstitutional Cybersecurity Board, provided for in Regulation (EU, Euratom) 2023/2841 [30].

A special place in the system is occupied by expert-analytical and research structures. The European Digital Media Observatory (EDMO) functions as a multidisciplinary platform that brings together scientists, fact-checkers, media literacy experts and regional hubs, providing research on disinformation, development of fact-checking and evidence-based support for public policy [38]. Its significance lies precisely in the formation of an independent analytical environment between regulatory policy, scientific expertise and civil society.

A new element of this block was the European Centre for Democratic Resilience, which began its work on February 24, 2026. The Centre was established within the framework of the European Democracy Shield as a platform for exchange between EU institutions, Member States and civil society to strengthen democratic resilience, protect the integrity of public debate and develop responses to common threats to democracy [39].

The main characteristic of the institutional and organizational model shown in Figure 4.1 is the absence of a single hierarchical center for information security management. Instead, there is a system of division of competences between institutions and specialized structures of the EU, within which each entity performs functions defined by regulatory acts, and their consistency is ensured by mechanisms for coordination and information exchange.

That is why the central part of the author's scheme reflects the main forms of interaction of the institutional-legal and institutional-organizational components: coordination, implementation, monitoring, information exchange, response and capacity development. At the EU level, they ensure the consistency of regulatory requirements and the activities of relevant institutions, and at the level of the Member States they are implemented by competent national authorities, regulators and response services. This approach makes it possible to consider the institutional support for EU information security not as a static set of regulatory acts and institutions, but as a system of interconnected legal and organizational mechanisms. The institutional-legal component establishes principles, rules and requirements, the institutional-organizational component ensures their practical implementation, and coordination mechanisms coordinate the activities of relevant entities. The result of the functioning of these components is the formation of a secure and stable information environment of the European Union, reducing vulnerability to information and cyber influences, protecting democratic processes and fundamental rights, strengthening citizens' trust, and ensuring safe conditions for the development of the digital economy.

Thus, the institutional framework for information security and digital resilience of the EU is characterized by a combination of different areas of legal regulation, a clear division of competences and a developed system of coordination between institutions. Their specificity lies not in the concentration of powers in one specialized

body, but in the complementarity of strategic documents, regulatory acts, regulatory mechanisms, specialized agencies, coordination networks and independent expert structures. It is this configuration that allows the European Union to simultaneously respond to technological, information, communication and hybrid threats, without separating them from the tasks of protecting democracy, fundamental rights and digital resilience.

4.2. Transformation of information threats to Ukraine and the EU in the context of hybrid and full-scale war

The modern security environment is characterized by the strengthening of the role of information influence as an independent and at the same time integrated tool of political, military and social confrontation. For Ukraine and the European Union, information threats have acquired particular importance in the conditions of prolonged hybrid aggression and full-scale war, since their impact is directed not only at information resources and digital infrastructure, but also at public trust, democratic processes, political stability and international interaction. In this context, among the key challenges and threats to the information security of Ukraine and the EU, it is appropriate to single out information warfare, information terrorism and information crimes (Fig. 4.2), which differ in forms of implementation and scale of influence, but have a common destructive focus.

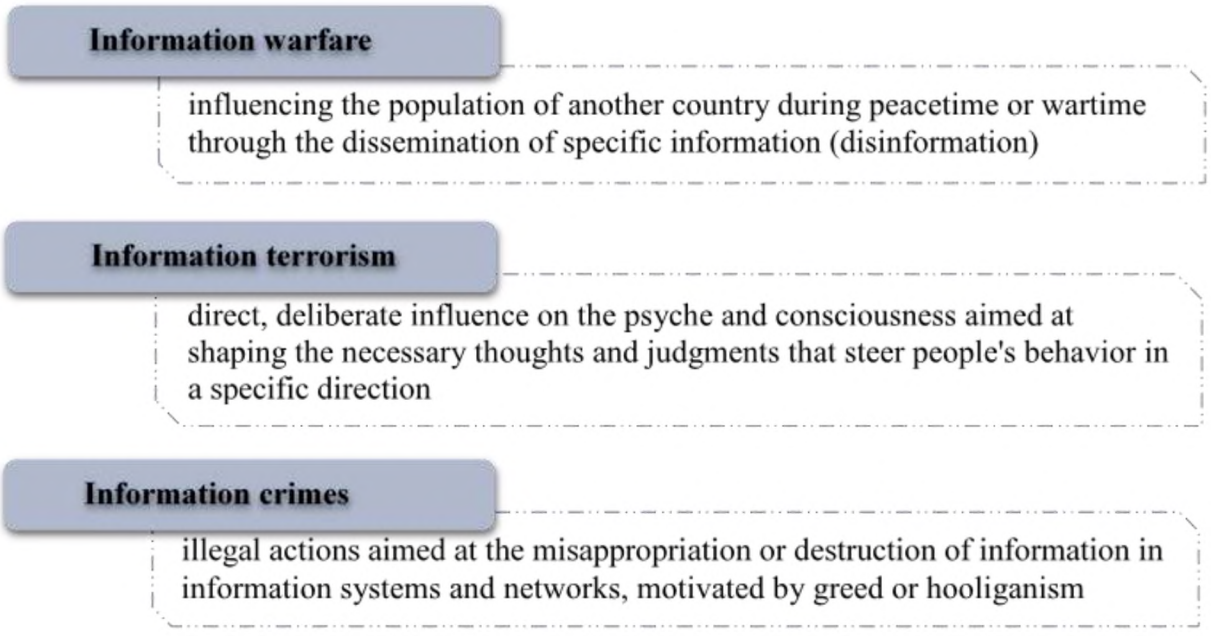


Fig. 4.2. Key challenges and threats to information security in Ukraine and the EU

Information warfare is a comprehensive strategy of influence aimed at achieving information superiority through information manipulation, its systematic disinformation and control over information channels. It includes both offensive and defensive operations aimed at creating and maintaining panic, destabilizing or conflict-generating narratives in the enemy's society, while simultaneously strengthening one's own information positions [40].

Information warfare uses all available means of the digital environment – from social media and messengers to traditional mass communication channels – to shape the perception of events and influence the decisions of key audiences. It is not only the propaganda of a certain political line, but also the systematic coordination of resources to create asymmetric information advantages in the conditions of hybrid conflicts. Such operations involve both technical network attacks and cyber campaigns to create and spread "fake" messages, manipulative messages and negative narratives, which significantly complicates their detection and neutralization in the international space.

Information warfare is based on 4D technology (Fig. 4.3).

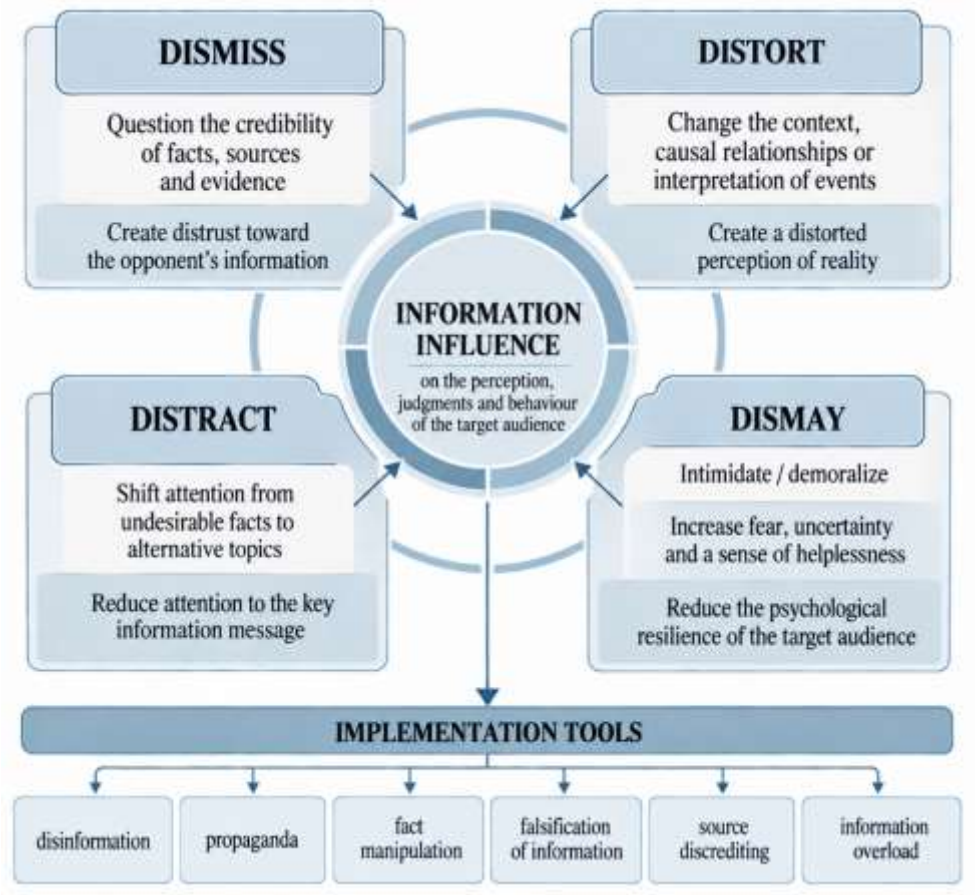


Fig. 4.3. Functional model of information influence 4D

Information warfare is one of the key components of modern hybrid conflicts. Aggressor countries, in particular the Russian Federation, actively use information and psychological operations to influence public opinion, undermine trust in democratic

institutions and promote their own geopolitical interests. These operations are implemented through manipulations in the media space, social networks and alternative information channels. In this context, the experience of the European Union in countering disinformation and strengthening the information resilience of states and citizens is particularly important.

Information terrorism is a phenomenon that goes beyond purely propaganda campaigns and takes on the characteristics of purposeful destructive activity with elements of intimidation, manipulation of consciousness and psychological pressure on wide audiences. As the Center for Countering Disinformation notes, this phenomenon arose as a result of the combination of global digitalization and the growing role of information technologies, which created a new "battlefield" for the enemies of democratic societies [41]. Information terrorism is aimed at destroying trust in institutions, increasing internal contradictions and weakening social cohesion through the deliberate dissemination of false or provocative messages.

This phenomenon includes cyberterrorism and media terrorism as separate forms of its implementation. Cyberterrorism is characterized by the use of digital technologies and network space to organize and carry out attacks that can disrupt the functioning of critical information infrastructure and cause panic or shock in society. Media terrorism is a directed information influence through mass media, social networks and other communication platforms with the aim of creating an atmosphere of fear or coercing public authorities to take certain actions. Such forms of terrorism are not always easily classified as traditional crimes, but they have a clear socio-psychological effect that can undermine the stability of society [42, 43].

Information terrorism is aimed not only at manipulating public opinion, but also at creating panic, destabilizing political processes and causing psychological pressure on individual social groups or entire societies. Analysis of such phenomena shows that such campaigns can use both traditional media and digital platforms, creating the illusion of mass support or opposition to certain political events [44]. In general, information terrorism is based on the following principles (Fig. 4.4).

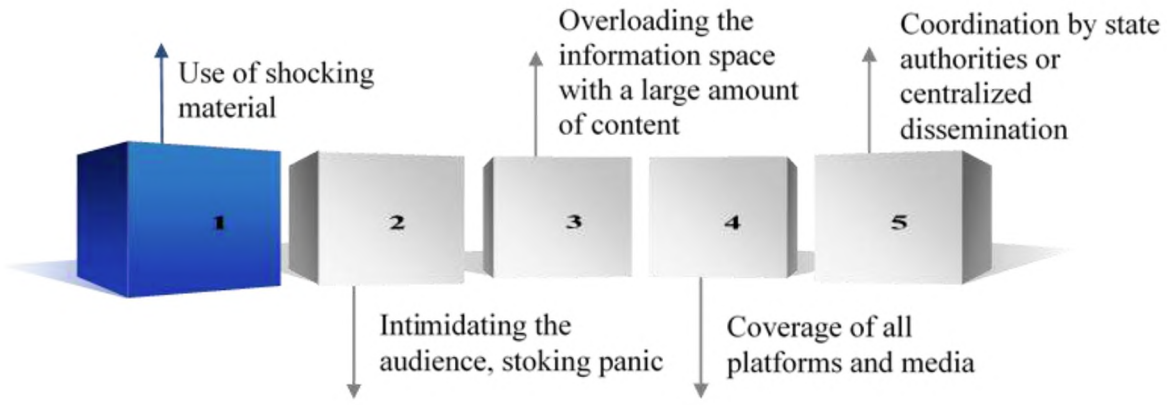


Fig. 4.4. Principles of information terrorism

It should be noted that information terrorism often coexists in the same information space with fake news as a form of disinformation, using similar distribution channels and technological means. However, they are not identical phenomena.

Information crimes constitute the third group of threats and encompass illegal actions in the digital environment aimed at obtaining, distorting or distributing information with the aim of causing harm to individuals, organizations or states. These include:

1) cyberattacks on information systems (database hacking, DDoS attacks) – such actions directly threaten the integrity and availability of information that is critical for ensuring the functioning of state and economic structures;

2) unauthorized access to data and information leaks, which may compromise strategic plans or citizens' personal data;

3) creation and distribution of malicious programs used to manipulate control systems or steal information.

These crimes often have a complex transnational nature, making them difficult to investigate in a digital environment. For example, digital bots and artificial accounts are increasingly used to automatically spread propaganda or manipulate social media, which not only exacerbates hybrid threats, but also creates new challenges for legal regulation and international cooperation to counter such forms of crime.

Taken together, the presence of these global threats requires the formation of a comprehensive approach to security, in which the information dimension is considered as a strategically important factor in ensuring the stability and effectiveness of the European Union's policy. The interdependence of information, political, military, economic and cyber threats was especially clearly manifested in the context of the Russian-Ukrainian war, the information dimension of which was formed long before the start of the full-scale invasion and gradually acquired a cross-border character. Starting from 2014, information influence has been increasingly closely combined with other tools of hybrid aggression, covering not only the information space of Ukraine, but also the Member States and institutions of the European Union. This gives grounds to consider information operations against Ukraine and the EU as an interconnected element of a broader system of hybrid influence.

For Ukraine, information threats have a direct impact on national security. The Information Security Strategy of Ukraine defines them as potentially or actually negative phenomena, trends and factors of information influence that can complicate the implementation of national interests and create risks for national security and defense [45]. The document emphasizes the systemic nature of external information influence aimed at undermining the sovereignty, democratic development, social consolidation and international positions of Ukraine.

At the same time, the experience of recent years shows that information threats associated with Russian aggression are not limited to the national information space of

Ukraine. They cover the EU Member States, European institutions, political parties, media and civil society. In European Union documents, the relevant activities are increasingly characterized through the category of Foreign Information Manipulation and Interference (FIMI), which allows us to focus not only on the falsity of a single message, but also on the coordination, intentionality, secrecy and strategic direction of the information operation. According to the European External Action Service, Ukraine has remained the main target of Russian FIMI operations in recent years, but at the same time the European Union, its Member States, NATO, the media and other public institutions are experiencing a large-scale impact [46]. This indicates the formation of a common space of information risks, within which the information influence on Ukraine and the EU is implemented as an interconnected process.

The full-scale invasion of February 24, 2022 was not the beginning, but a qualitatively new stage in the transformation of information threats to Ukraine. Information operations began to be more actively synchronized with military operations, cyberattacks, diplomatic pressure, economic instruments, and attempts to influence public opinion in European countries. As a result, not only the intensity of information threats changed, but also their structure: target audiences expanded, the number of distribution channels increased, the infrastructure of information influence became more complicated, and individual disinformation messages increasingly became elements of long-term and coordinated campaigns.

This trend is particularly evident in attempts to influence the attitude of European societies towards supporting Ukraine. Russian information campaigns are aimed at spreading ideas about the excessive cost of aid to Ukraine, discrediting Ukrainian statehood, increasing social polarization, forming distrust of European institutions, and presenting the war as a consequence of the policies of the EU or Ukraine itself. In this way, the information influence on the European audience simultaneously performs two tasks: it weakens the internal stability of the EU and creates the prerequisites for reducing political, financial, and military support for Ukraine.

The above allows us to state that modern information threats to Ukraine and the European Union have a common strategic origin, but differ in their direct objects and mechanisms of influence. For Ukraine, the priority objects remain statehood, defense capability, public trust, European integration and international support; for the EU – democratic institutions, electoral processes, social cohesion, trust in supranational and national authorities and readiness to continue supporting Ukraine.

That is why it is advisable to analyze the transformation of information threats not only in a chronological dimension, but also through changes in their key characteristics: scale, implementation technologies, target audiences, distribution methods, and degree of integration with other tools of hybrid influence.

Further analysis provides grounds to consider the transformation of information threats to Ukraine and the European Union as a sequential process, within which not only the intensity and scale of information influence changed, but also the methods of its organization, distribution technologies, the composition of target audiences and the nature of interaction with other instruments of hybrid influence. On this basis, it is advisable to distinguish three stages of the transformation of information threats: the formation of a systemic model of hybrid information influence (2014–2021); scaling and cross-border integration of information operations in conditions of full-scale war (2022–2024); technologization, networking and adaptive targeting of FIMI operations (2025–2026). The identified stages are systematized in Figure 4.5.

The beginning of Russian aggression against Ukraine in 2014 was a period when information tools finally became an integral part of a broader hybrid strategy. Their use was aimed not only at spreading individual unreliable messages, but also at forming stable interpretations of events, delegitimizing Ukrainian statehood, justifying aggressive actions, and creating distrust in Ukraine's European and Euro-Atlantic course.

A characteristic feature of the first stage (see Fig. 4.5) was the combination of traditional propaganda with digital channels of content distribution. Information messages were broadcast through controlled media, social networks, pseudo-news resources and anonymous information platforms. At the same time, a significant part of the narratives had a long-term nature and were not tied to a single information event. Their repetition formed stable patterns of perception of Ukraine as a "failed state", questioned its European choice and were used to justify Russian policy.

At the regulatory level, the systemic nature of such threats was recorded in the Information Security Strategy of Ukraine 2021, which directly identified countering disinformation and information operations of the aggressor state as one of the priorities of state policy [45]. The document also linked information aggression to risks to state sovereignty, territorial integrity, democratic constitutional order, and European and Euro-Atlantic integration of Ukraine.

For the European Union, this period also became a stage of rethinking the nature of external information influence. Gradually, the problem of disinformation began to be viewed not only as a question of media literacy or the reliability of information, but as an element of a broader hybrid influence that can influence democratic processes, public opinion and foreign policy decisions. It was during this period that the institutional foundations of European counter-disinformation were laid, which later transformed into a more comprehensive approach to FIMI.

Thus, the first stage was characterized by the formation of a stable model of information influence, within which individual propaganda messages gradually turned into systemic narrative campaigns, and the information component became a permanent tool of hybrid pressure on Ukraine and the European information space.

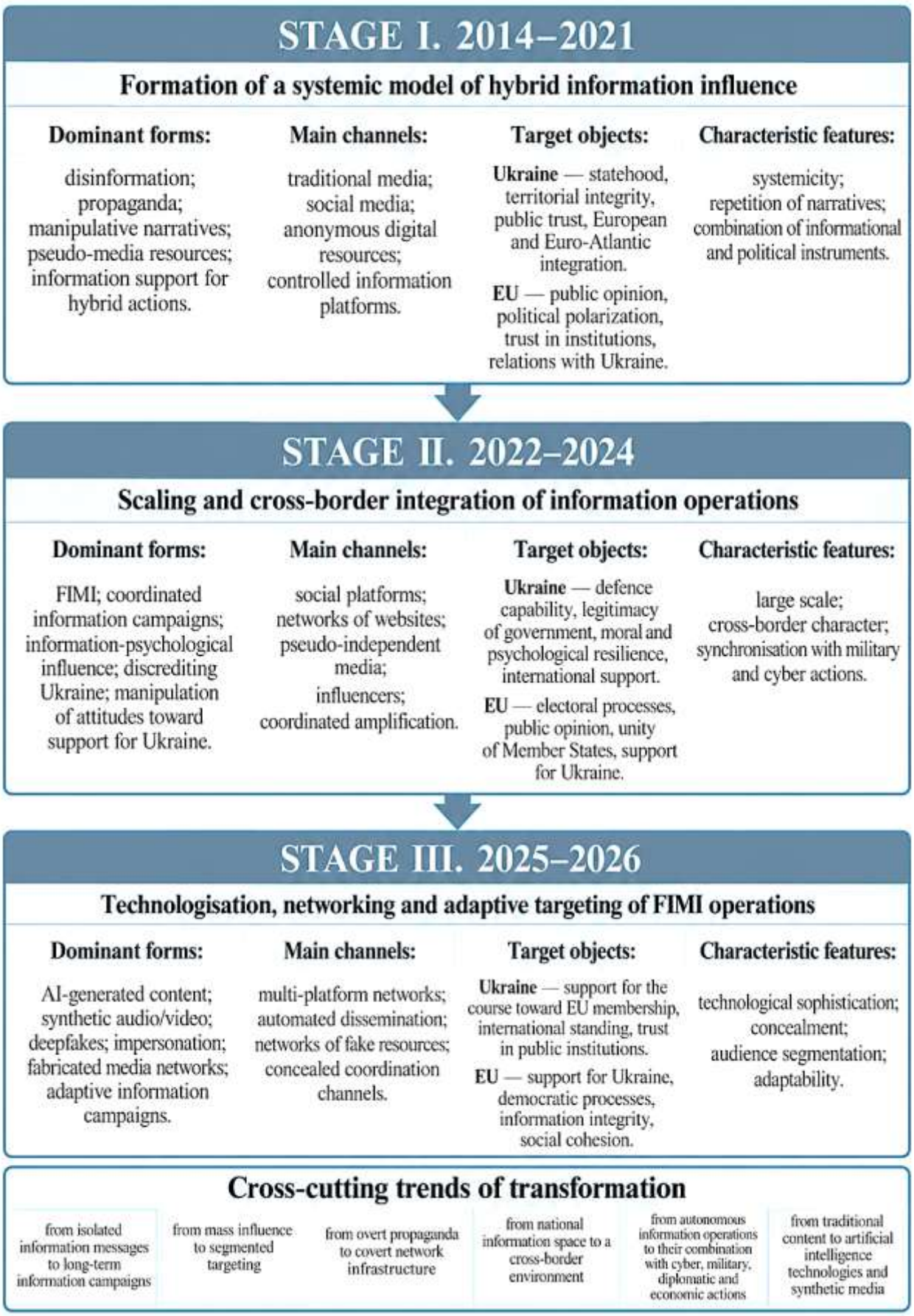


Fig. 4.5. Stages of transformation of information threats to Ukraine and the European Union

Russia's full-scale invasion of Ukraine on February 24, 2022 significantly changed the scale and functions of information operations. If before that, information influence mainly accompanied hybrid actions, then in the conditions of a full-scale war it began to be directly integrated with military, cyber, diplomatic and economic means. Information campaigns began to target several groups of audiences simultaneously. Inside Ukraine, they were aimed at weakening trust in state authorities, the Armed Forces of Ukraine, international partners and the state's ability to resist. In European countries, the emphasis shifted to discrediting support for Ukraine, exaggerating its economic value for EU citizens, increasing public polarization and raising doubts about the appropriateness of sanctions and military assistance.

It was during this period that the category of Foreign Information Manipulation and Interference became key to the analysis of external information interference at the EU level. The second EEAS report on FIMI threats demonstrated that Ukraine remained one of the main targets of the operations studied, while their content was simultaneously aimed at European audiences and support for Ukraine from EU member states [46].

In 2024, the EEAS recorded a further strengthening of this trend. Ukraine remained the main target of Russian FIMI operations; a significant part of the information activity was aimed at delegitimizing the Ukrainian authorities, reducing international support and justifying Russian aggression. At the same time, campaigns against the EU focused on migration, the cost of living, discrediting European leaders and electoral processes. A separate trend was the more intensive use of content created with the help of artificial intelligence [47].

The cross-border nature of the threats is also confirmed by the practice of the EU Council. In October 2024, the European Union directly characterized Russian activities as a broad hybrid campaign, including cyberattacks, information manipulation and interference, sabotage and actions against critical infrastructure [48]. An illustrative example was also the application of sanctions against individuals and structures involved in international information manipulation campaigns. In particular, in May 2024, the EU Council noted that Voice of Europe was carrying out a systematic international media manipulation campaign with the aim of destabilizing Ukraine, the EU and its member states [49].

Thus, in 2022–2024, information threats have acquired a distinctly cross-border and integrated nature. Their strategic feature has been the simultaneous focus on two interrelated goals: weakening Ukraine's internal stability and reducing Ukraine's external support from the European Union.

Starting from 2025, the technological and network dimension of information threats is increasingly evident. It is not only about increasing the number of information messages, but also about improving the methods of their creation, masking, distribution and adaptation to specific audiences. EEAS reports indicate the growing role of networks of sites and accounts, coordinated distribution of content, substitution of information sources and the use of synthetic media. In the fourth EEAS report on FIMI

2026, Ukraine is again identified as one of the main objects of Russian information influence, and among the main goals of such operations are the reduction of international support for Ukraine and the formation of the perception of Ukraine as a source of threats or provocations [50].

It is important that the transformation concerns not only technologies, but also thematic targeting. In 2025–2026, a separate direction was taken by campaigns aimed directly at discrediting Ukraine's European integration. A joint report by the EEAS and the Center for Countering Disinformation under the National Security and Defense Council of Ukraine, published in June 2026, analyzes Russian FIMI operations for the period from January 2025 to May 2026, the purpose of which was to weaken domestic support for Ukraine's accession to the EU [51]. This indicates a shift to more adaptive information influence, when the content of campaigns is determined not only by general strategic goals, but also by current political processes. Information operations are increasingly adapting to specific negotiations, decisions, election campaigns, crisis events or socio-economic problems. At the same time, the distribution infrastructure is changing. In place of individual large information resources, networks of interconnected sites, accounts, pseudo-media platforms and distribution channels are taking their place, which creates more complex conditions for establishing the primary source of information influence. This reinforces the importance of behavioral analysis, research into coordination between participants in information campaigns and the identification of network connections - precisely the approaches that form the basis of the modern FIMI methodology.

In July 2025, the Council of the EU imposed restrictive measures against individuals and entities involved in Russian destabilizing actions in Ukraine and the European Union. Among other things, the use of Russian broadcasting infrastructure in the temporarily occupied territories of Ukraine to replace Ukrainian broadcasting with Russian-controlled content was recorded [52].

Thus, the third stage is characterized not simply by an increase in the scale of information influence, but by its qualitative technological transformation. The main features are the use of artificial intelligence and synthetic content, the network nature of the distribution infrastructure, hiding sources, segmented targeting, and operational adaptation of content to political and social processes in Ukraine and the EU.

A comparison of the three stages allows us to establish a general pattern: the transformation of information threats is taking place in the direction of increasing their technological sophistication, cross-border nature, coordination and integration with other instruments of hybrid influence. If at the first stage the main task was to form and consolidate destructive narratives, then in the conditions of a full-scale war information operations have become an integral part of broader destabilizing campaigns, and in 2025–2026 they are increasingly acquiring the features of technologically sophisticated, network-organized and adapted to specific audiences FIMI operations.

At the same time, Ukraine and the European Union are increasingly in a common space of information threats. The destabilization of Ukraine is used as a means of influencing European security, while information pressure on EU member states is aimed, among other things, at weakening support for Ukraine. It is this interdependence that makes it necessary to further develop joint mechanisms for identifying, analyzing and countering information threats.

4.3. Strategic partnership between Ukraine and the European Union in the field of cybersecurity: institutional mechanisms and development directions

Deepening digital interdependence, the growth of cross-border cyber threats and the use of cyber operations as a component of hybrid and full-scale warfare have led to a significant strengthening of the cybersecurity dimension of relations between Ukraine and the European Union. For Ukraine, such cooperation has a dual meaning. On the one hand, it provides access to European expertise, technological and organizational support, mechanisms for responding to cyber incidents and building national capabilities. On the other hand, approximation to the regulatory and organizational principles of EU cybersecurity is part of the broader process of Ukraine's European integration and its gradual inclusion in the common digital and security space.

Russian aggression has significantly accelerated this process. Cyberattacks against state information resources, critical infrastructure, telecommunications systems, and the private sector have demonstrated that cybersecurity in wartime directly affects the continuity of state administration, the functioning of the economy, defense capability, and social stability. Scientific studies also emphasize that the modern cybersecurity system of Ukraine is developing simultaneously under the influence of two factors – the need to counter military cyber threats and the need to approach European norms and practices [53, 54].

At the same time, the modern partnership between Ukraine and the EU in the field of cybersecurity can no longer be reduced exclusively to providing assistance to a state at war. Its content is gradually expanding through political dialogue, regulatory approximation, institutional interaction, exchange of information about threats, development of joint response procedures, training of specialists, cyber diplomacy and involvement of Ukraine in certain mechanisms of cyber solidarity of the EU. It is the combination of these areas that gives grounds to consider cooperation in the field of cybersecurity as an important component of the strategic partnership between Ukraine and the European Union. The main institutional mechanisms of such a partnership and the directions of its further development are systematized in Figure 4.6.

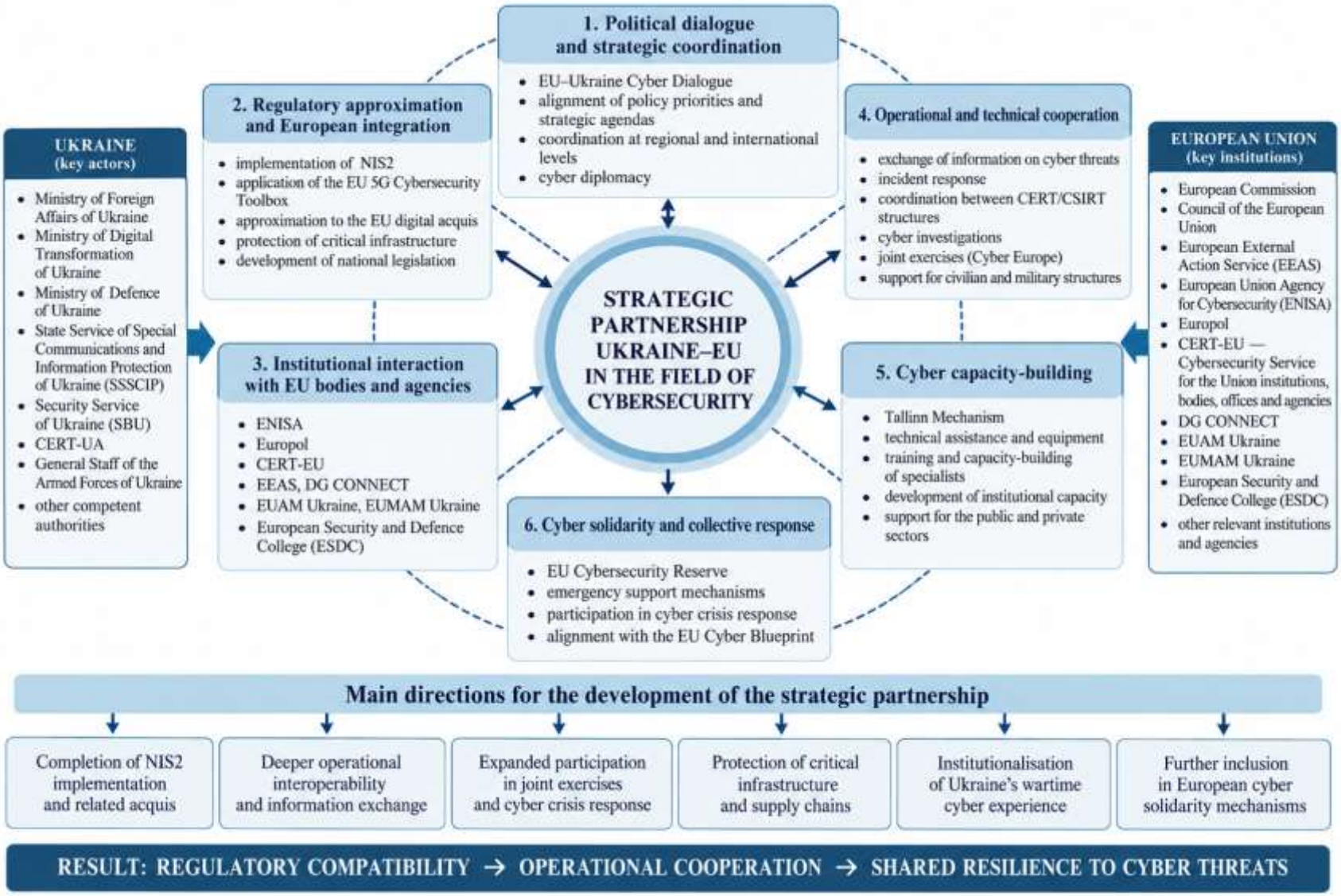


Fig. 4.6. Institutional mechanisms of strategic partnership between Ukraine and the EU in the field of cybersecurity

Source: developed based on [55–65]

As can be seen from Figure 4.6, the strategic partnership between Ukraine and the EU in the field of cybersecurity is implemented through a set of interrelated mechanisms, namely political dialogue and strategic coordination, regulatory approximation, institutional interaction, operational and technical cooperation, cyber capability building, as well as mechanisms of cyber solidarity and collective response.

The central policy-coordination mechanism for such cooperation has become the EU–Ukraine Cyber Dialogue, which has been held since 2021 and has gradually turned into a permanent platform for coordinating positions on cyber threats, legislative changes, cyber diplomacy and practical interaction. The third cyber dialogue, held on July 15, 2024 in Brussels, took place after the opening of negotiations on Ukraine's accession to the EU, which gave the cooperation additional integration content. The parties discussed the approximation of Ukrainian legislation to NIS2, digital product security and certification, protection of critical infrastructure and supply chains, situational awareness, cyber crisis management, the application of the EU Cyber Diplomacy Toolbox, the development of cooperation with ENISA and Europol, as well as the possibility of Ukraine's access to the EU Cybersecurity Reserve [55].

Further deepening of these areas took place during the fourth EU–Ukraine Cyber Dialogue, held on October 16, 2025 in Kyiv. A feature of this stage was that the subject of discussion was not only current threats and support for Ukraine's cyber resilience, but also closer coordination of cybersecurity policy with the EU acquis, including the implementation of the digital section of the Ukraine Plan, the implementation of NIS2, the full implementation of the EU 5G Cybersecurity Toolbox and approximation to the EU policy in the field of cyber defense [56]. The parties paid special attention to practices of deterrence and response to cyber attacks, sanctions mechanisms, investigation of cybercrimes, capacity building and further access of Ukraine to reserve European response mechanisms.

Thus, the Cyber Dialogue performs several functions at once. First, it ensures political coordination of bilateral cooperation. Second, it coordinates regulatory changes. Third, it serves as a platform for identifying specific operational areas of cooperation between competent authorities. Fourth, the dialogue links the Ukraine–EU bilateral format with broader international mechanisms of cyber diplomacy, in particular activities in the UN and OSCE [56].

An important institutional basis for practical cooperation was the conclusion in November 2023 of the Working Arrangement between ENISA, the National Cybersecurity Coordination Center of Ukraine and the State Special Communications Administration. This arrangement was the first such agreement concluded by ENISA with a partner outside the EU, which demonstrates the special nature of cooperation with Ukraine [57]. The identified areas include cyber capacity building, exchange of best practices, participation in exercises, awareness raising, convergence of approaches

to the implementation of legislation, in particular NIS2, as well as systematic exchange of information to enhance common situational awareness.

It is the interaction with ENISA that is indicative of the transition from external technical assistance to institutional rapprochement. It is no longer just about the transfer of equipment or conducting individual training events, but about the gradual harmonization of risk assessment methodologies, response procedures, personnel training and approaches to state regulation of cybersecurity. The updated ENISA 2025 international strategy maintains cooperation with Ukraine among the priority areas of the Agency's international activities and provides for the adaptation of the Working Arrangement to changing needs and the nature of cyber threats [58].

The second fundamental direction of the partnership is the regulatory and legal approximation of Ukraine with the cybersecurity system of the European Union. In this context, Directive (EU) 2022/2555 – NIS2, which establishes a common legal framework for cyber risk management for critical and important EU entities, is of decisive importance. For Ukraine, its implementation is not only a matter of improving the national cybersecurity system, but also a component of fulfilling European integration obligations.

This direction is directly enshrined in the Plan of Ukraine within the Ukraine Facility. In particular, the reform "Secure and Efficient Digital Infrastructure" provides for the approximation of Ukrainian legislation to the NIS/NIS2 framework and the creation of prerequisites for the implementation of the EU 5G Cybersecurity Toolbox [59]. In March 2025, the Verkhovna Rada of Ukraine adopted Law No. 4336-IX on the Protection of State Information Resources and Critical Information Infrastructure Facilities, which entered into force on April 18, 2025. In 2025, the European Commission confirmed the implementation of the relevant stage of the Plan of Ukraine and noted that the legislative changes take into account the principles of NIS2 [60].

At the same time, the process of regulatory convergence is not complete. In the Ukraine Report 2025, the European Commission noted a significant strengthening of the Ukrainian regulatory and institutional framework for cybersecurity, but at the same time emphasized that a number of provisions of the EU acquis still need to be fully implemented to ensure compliance with NIS2. It specifically noted the need to further implement the EU 5G Cybersecurity Toolbox and address the risks associated with the use of high-risk vendors [61]. Therefore, regulatory integration should be seen as a long-term process that encompasses not only the formal transfer of norms, but also ensuring the effectiveness of risk management, supervision, incident reporting and liability procedures.

This conclusion is also confirmed by modern Ukrainian studies, which link Ukraine's integration into the European cybersecurity system with the harmonization of legislation, strengthening the protection of critical infrastructure, development of

certification and improvement of organizational coordination [54]. The scientific discourse emphasizes that the implementation of NIS2 requires not only legislative changes, but also sufficient institutional capacity, a clear division of competences and an effective oversight mechanism [62].

Along with regulatory convergence, operational and technical cooperation is deepening. The parties regularly exchange information on the development of cyber threats, practices for detecting and responding to incidents, assessing cyber risks, and experience in managing cyber crises. In this direction, an important role is played by ENISA, Europol, CERT-EU, and Ukrainian competent authorities, primarily the State Service for Special Communications, CERT-UA, the National Cybersecurity Coordination Center, the Security Service of Ukraine, and other entities of the national cybersecurity system [55–57]. Evidence of the gradual expansion of practical cooperation was Ukraine's involvement in Cyber Europe 2026, a large-scale EU exercise on responding to cyberattacks against railway and maritime infrastructure. About 5,000 experts, including representatives of Ukraine as a partner state, participated in the exercise, organized by ENISA on June 10–11, 2026. For the first time, the provisions of the EU Cyber Blueprint 2025 and the Cybersecurity Reserve mechanisms were also tested within the framework of such exercises [63]. Ukraine's participation in such events is important not only for acquiring practical skills, but also for gradually harmonizing crisis response procedures with European ones.

A separate area of cooperation is cyber capacity building, which is carried out both through bilateral EU mechanisms and within the framework of broader partnership initiatives. An important place belongs to the Tallinn Mechanism, established in December 2023 to coordinate civilian assistance to Ukraine in the field of cybersecurity. The mechanism brings together eleven donor states, and the European Union and NATO support its activities. Its purpose is to coordinate short-term technical support and long-term capacity building, including equipment, training and support for responding to cyber incidents [64]. The significance of the Tallinn Mechanism also lies in reducing the fragmentation of international assistance. For Ukraine, which simultaneously interacts with a large number of states and international organizations in the field of cybersecurity, coordination of needs and resources is of fundamental importance to avoid duplication of projects, ensure compatibility of solutions and direct support to the most critical areas. In this sense, the EU's participation in the Tallinn Mechanism complements the bilateral Cyber Dialogue with practical tools for implementing the identified priorities.

A qualitatively new stage of cooperation began in 2026, when Ukraine was given the opportunity to use the EU Cybersecurity Reserve. On June 15, 2026, the European Commission announced that, following a relevant decision by the EU Council, Ukraine may activate emergency support to the Reserve in the event of significant or large-scale

cyber incidents [65]. The mechanism, established under the Cyber Solidarity Act and managed by ENISA, provides for the provision of incident response services by verified private providers. This event is of fundamental importance for assessing the nature of the partnership. While early forms of cooperation were mainly based on the EU's support for Ukraine's cyber resilience, access to the Cybersecurity Reserve indicates Ukraine's gradual involvement in common European cyber crisis response mechanisms. At the same time, this does not yet mean full institutional integration into the EU cybersecurity system: the legal status of a candidate country and the scope of access to individual mechanisms differ from the capabilities of the Member States. Therefore, it is more correct to talk about the gradual expansion of interoperability and Ukraine's participation in certain EU mechanisms.

An equally important characteristic of the strategic partnership is its bilateral, rather than purely donor, nature. Ukraine receives regulatory, financial, technical and expert support, but at the same time provides the European Union with unique experience in countering large-scale state cyber operations in real war conditions. Ukrainian competent authorities possess a significant amount of information on the tactics, techniques and procedures of Russian cyber groups, mechanisms for combining cyber attacks with information and military operations, as well as practical models for ensuring the continuity of the functioning of state digital systems. During the EU–Ukraine Cyber Dialogues, the parties repeatedly emphasized the need to exchange experience, situational information and threat assessments [55, 56]. The Working Arrangement with ENISA also directly provides for the mutual exchange of knowledge and information to increase joint situational awareness [57]. Thus, Ukraine's experience is gradually becoming an additional source of increasing the EU's own readiness to counter state and state-related cyber threats.

Thus, it is legitimate to note the modern understanding of cybersecurity as an area where the effectiveness of national systems largely depends on international data exchange, coordination between the state and the private sector, and the ability to quickly use the practical experience of partners. A study of public-private interaction in Ukraine during a full-scale war shows that the combination of national resources with the support of partner states and private technology companies has become one of the factors increasing Ukrainian cyber resilience [66].

Along with operational interaction, cyber diplomacy is gaining importance. Ukraine and the EU support a common vision of the applicability of international law to cyberspace, adherence to the framework of responsible state behavior developed within the UN, and the need to hold actors accountable for malicious activity in cyberspace [55, 56]. A practical tool for this policy is the EU Cyber Diplomacy Toolbox, which combines diplomatic, political, and sanctioning means of responding to significant cyber incidents. For Ukraine, this area is important not only as a

mechanism for responding to Russian cyberattacks, but also as an opportunity to integrate its own experience in attribution and documentation of cyber incidents into a broader system of collective international response.

Further development of the strategic partnership requires solving a number of tasks. First of all, it concerns completing the implementation of the provisions of NIS2 and related acquis, ensuring the practical effectiveness of legislative changes and strengthening the capacity of competent authorities to carry out risk-based supervision. The European Commission in its 2025 report explicitly states that, despite significant progress, full approximation to NIS2 has not yet been achieved [61].

The second direction is to deepen interoperability. Expanding regular information exchange between CERT/CSIRT structures, Ukraine's participation in joint exercises, developing procedures for responding to cross-border cyber incidents, and gradually bringing national crisis management closer to the EU Cyber Blueprint approaches seem promising.

The third direction should be further institutional rapprochement with ENISA and other EU cybersecurity structures. The Working Arrangement practice demonstrates the possibility of systemic cooperation even before full membership. It is advisable to expand the participation of Ukrainian specialists in training programs, expert groups, crisis scenario modeling and joint threat assessments.

The fourth area is related to the protection of critical infrastructure and ICT supply chains. European policy is increasingly focused not only on the protection of individual information systems, but also on the risks arising from dependence on technology suppliers, software, telecommunications equipment and other elements of digital supply chains. For Ukraine, this area is particularly relevant in the context of the restoration of critical infrastructure and further integration into the EU's single digital market.

The fifth direction is the institutionalization of the exchange of military experience of Ukraine. Knowledge gained in the conditions of constant cyberattacks should not only be situationally transferred to partners, but also systematized and included in joint exercises, methodological documents, incident response models and assessment of new types of threats. This will allow to strengthen not only the cyber resilience of Ukraine, but also the readiness of the European Union for complex hybrid scenarios.

Finally, a promising direction is the further inclusion of Ukraine in the mechanisms of European cyber solidarity. Access to the EU Cybersecurity Reserve obtained in 2026 demonstrates the possibility of such an approach [65]. In the long term, the strategic partnership should focus on the maximum possible compatibility of Ukraine's procedures, standards and response mechanisms with the European cybersecurity system before membership.

Thus, the strategic partnership between Ukraine and the European Union in the field of cybersecurity is at the stage of transition from a model of support to a model of gradual integration. Political cyber dialogue is complemented by regulatory convergence, structured interaction with ENISA and Europol, coordination of international assistance through the Tallinn Mechanism, participation in joint exercises and access to the EU Cybersecurity Reserve. At the same time, Ukraine is increasingly acting not only as a recipient of support, but also as a partner whose practical experience in countering state cyberattacks is of direct importance for strengthening the cyber resilience of the European Union. The strategic outcome of the further development of the partnership should be the achievement of regulatory compatibility, deepening operational cooperation and the formation of a joint capacity of Ukraine and the EU to prevent, detect and neutralize cross-border cyber threats.

4.4. Digital integration of Ukraine into the European Union: security imperatives, risks and strategic prospects

The development of cooperation between Ukraine and the European Union in the field of information and cybersecurity, discussed in the previous sections, indicates a gradual transition from individual formats of sectoral interaction to a much broader process of digital integration. Its content is no longer limited to issues of cyber defense or exchange of information about threats, but covers electronic communications, digital services, electronic identification and trust services, personal data protection, interoperability of state digital systems, open data, artificial intelligence, the media environment and other components of the EU digital acquis. In the European Commission's 2025 report, digital transformation and media are singled out as an independent negotiating chapter 10, and Ukraine is assessed as being between a moderate and good level of preparation in this area [61]. Under such conditions, it is advisable to consider Ukraine's digital integration into the EU not as a continuation of internal digitalization, but as a process of regulatory, institutional, technological and market convergence with the digital environment of the European Union, the result of which should be the compatibility of rules, digital infrastructures, services and security mechanisms and the gradual inclusion of Ukraine in the relevant segments of the EU internal market. Such an approach is consistent with modern studies of Ukraine's integration into the digital single market, where its main components are defined as regulatory approximation, removal of cross-border barriers, development of digital infrastructure and adaptation of business and public services to European rules [76–78].

It is fundamentally important to distinguish between the concepts of "digital transformation" and "digital integration". The first characterizes internal changes in the ways of organizing public administration, economic processes, communications and service provision under the influence of digital technologies. The second involves not only modernization within the country, but also achieving compatibility with the external regulatory and institutional environment of the EU. That is why digital integration includes not only technological updating, but also the adaptation of legislation, changing regulatory practices, ensuring mutual recognition of digital tools, integrating infrastructures and building the capacity to implement European rules in practice.

After Ukraine received the status of candidate country for EU accession, the relevant process acquired a new meaning. In the Ukraine Report 2025, the European Commission records the simultaneous progress of Ukraine in the field of roaming, electronic communications, open data, electronic identification and cybersecurity, but at the same time points to incomplete compliance with a number of provisions of the acquis, in particular with regard to the Digital Services Act, Digital Markets Act, Data Governance Act, NIS2, European Media Freedom Act, AI Act and European 5G security requirements [67]. One of the most significant results of practical digital integration was the extension of the Roam Like at Home regime to Ukraine. From January 1, 2026, citizens of Ukraine and EU Member States were able to use voice services, SMS and mobile data while staying in the EU or Ukraine, respectively, without additional roaming charges. The European Commission directly characterizes this as an important stage of Ukraine's gradual integration into the EU internal market [69].

The basis for such rapprochement was created gradually. In 2022, the Ukrainian regulator of electronic communications was given the opportunity to participate in the work of the Body of European Regulators for Electronic Communications (BEREC), including joining working groups on roaming, market regulation and broader digital policy [70]. In the same year, Ukraine was associated with the Digital Europe Programme, which opened up access to competitions in the fields of supercomputing, artificial intelligence, digital skills and other advanced digital technologies for Ukrainian enterprises, organizations and public administrations [68].

Thus, actual integration unfolds simultaneously in several planes: regulatory, institutional, technological, infrastructural and programmatic-financial. That is why its security component cannot be considered as auxiliary. In the context of growing interdependence of digital systems, expanding access to shared services and infrastructures simultaneously increases the potential consequences of vulnerabilities, cyberattacks, failures, technological dependencies and data compromise. Security in

this context is not a separate area of digital integration, but a prerequisite for its functional viability.

The first security imperative is regulatory compatibility with the EU digital acquis. Its significance lies not only in the formal transposition of European norms, but also in ensuring common rules for risk management, liability of digital platforms, data protection, electronic identification, cybersecurity and supervision. Ukraine has already taken initial steps towards approximation to the DSA, DMA and P2B Regulation, however, as of 2025, the European Commission has stated the need to continue preparing relevant legislation and identifying competent authorities [61]. Approximation to the European Digital Identity Framework. Regulation (EU) 2024/1183 provides for the creation of European digital wallets and forms a framework for secure cross-border access to public and private services, mutual recognition of digital identification and electronic attributes [71]. For Ukraine, this direction has a practical basis: according to the Commission's assessment, the Diia platform already met or exceeded the relevant eIDAS requirements in 2023, and the Ukrainian eIDAS Node operator received ISO/IEC 27001 certification in June 2025 [61]. At the same time, full compatibility still requires resolving certain issues, in particular, the certification of qualified electronic signature creation tools.

The second imperative is the cyber resilience of digital infrastructure. The expansion of digital services and cross-border interaction increases the dependence of the state, business and citizens on the continuity of the functioning of telecommunications networks, state registries, cloud services, electronic identification systems and critical information infrastructure. That is why the Ukraine Plan separately provides for the reform "Secure and efficient digital infrastructure", the purpose of which is to strengthen cybersecurity in the process of digital transformation, approach to NIS/NIS2 and create prerequisites for the implementation of the EU 5G Cybersecurity Toolbox [72].

The third imperative is the security of technological supply chains and the reduction of critical dependencies. This direction is of particular importance in the context of the European Union's rethinking of its own technology policy. In 2026, the Commission formulated an expanded concept of technological sovereignty, linking it to the EU's ability to control key technologies, data and infrastructure and reduce excessive dependence on external suppliers [74]. Separately, the NIS Cooperation Group approved the ICT Supply Chain Security Toolbox, which is focused on identifying, assessing and minimizing cyber risks in supply chains, including dependence on high-risk suppliers [75]. It should be noted that digital integration involves not only expanding access to technologies, but also changing the criteria for their selection: along with cost and functionality, security, controllability of supply

chains, the possibility of updating, certification and risks of external technological dependence become decisive.

The fourth imperative is data protection, digital rights and trust. The increase in cross-border digital interaction creates a need for compatibility of data processing rules, user identification and privacy protection. The European model of digital integration fundamentally combines the development of services with the requirements for the protection of personal data and user control over digital identity. Regulation (EU) 2024/1183, for example, provides not only for the technical interoperability of the European Digital Identity Wallet, but also for specific guarantees of data minimization, information separation and protection against unauthorized use [71].

The fifth imperative is the institutional capacity to ensure the practical application of the acquis. Formal compliance with legislation does not guarantee its effectiveness without sufficient human, financial and organizational capacity of regulators. The Ukraine Report 2025 explicitly identifies among its priority recommendations the adequate funding and staffing of independent telecommunications and media regulators, as well as central executive bodies in the field of electronic communications [61].

These imperatives allow us to consider digital integration as a process that simultaneously creates new opportunities and generates new risks. The most obvious of these is the risk of regulatory gap – a situation in which legislative approximation occurs faster than the formation of a real capacity to ensure the implementation of new rules. This is the risk that may arise in the areas of DSA, AI Act, Data Governance Act or NIS2, where the effectiveness of regulation depends on the availability of specialized bodies, oversight procedures, accountability mechanisms and expert resources. The second risk is associated with the growth of technological dependence. Integration into the European digital market opens up access to technologies and services, but at the same time can deepen dependence on foreign cloud platforms, suppliers of telecommunications equipment, components, software and computing infrastructure. This problem is not specific only to Ukraine: in the State of the Digital Decade 2026, the European Commission notes the preservation of significant dependencies of the EU itself in the field of semiconductors, cloud services, cybersecurity, and other strategic technologies [73].

It should be noted that the surface of cyberattacks is expanding. The more interconnected state registries, digital identification systems, telecommunications networks, business platforms and cross-border services become, the greater the consequences of compromising a single element. For Ukraine, this risk is exacerbated by war conditions, in which digital infrastructure simultaneously performs civil, economic and security functions. In addition, there is uneven adaptation of businesses and territories to new digital requirements. Approximation to the acquis creates

opportunities for access to the EU digital market, but at the same time requires additional costs for compliance, cybersecurity, data protection, certification and modernization of information systems. For small and medium-sized enterprises and entities with a lower level of digital maturity, the corresponding costs can be significant. Studies of Ukraine's digital integration confirm that the expected benefits of access to the Digital Single Market depend precisely on the ability of businesses to adapt to new regulatory and technological requirements [76, 77].

Another constraint is the shortage of digital skills and expertise. This problem is also common in the EU: the State of the Digital Decade 2026 notes that the share of ICT specialists remains significantly below the 2030 target, and the lack of skills limits the implementation of AI, cloud technologies and cybersecurity solutions [73]. For Ukraine, the human resources challenge is further exacerbated by migration, mobilization, competition for highly skilled professionals and the need to simultaneously ensure military cyber resilience and integration with European standards.

A special group is made up of information risks of digital integration itself. As shown in section 4.2, Ukraine's European course is the object of external information operations. Therefore, each deepening of digital integration - from the implementation of European regulation to participation in common digital infrastructures - may be accompanied by campaigns aimed at discrediting the relevant reforms, exaggerating their cost, spreading claims about the "loss of digital sovereignty" or distrust of European institutions. This means that communication support for reforms and information resilience should be components of digital integration policy.

At the same time, the presence of risks does not reduce the strategic potential of digital integration. On the contrary, gradual inclusion in the European digital environment can become one of the mechanisms of post-war recovery, productivity development, modernization of public administration and increasing business competitiveness. In the scientific literature, Ukraine's integration into the Digital Single Market is considered as a factor in reducing regulatory barriers to digital trade, the development of electronic services and accelerating the digitalization of the economy [76; 82]. The strategic direction of further integration should be the consistent completion of regulatory approximation under negotiating chapter 10 "Digital transformation and media". In this case, priority should be given not to the number of formally transposed acts, but to the degree of actual compatibility of regulatory procedures, technical standards and institutional practice. It is important to expand Ukraine's actual participation in European digital institutions, programs and infrastructures. The experience of BEREC, the Digital Europe Programme and Roam Like at Home proves that functional integration of individual sectors is possible even before full membership [68–70]. Such a format could become a model for the gradual

inclusion of Ukraine in other EU mechanisms, provided that the necessary level of regulatory and technical readiness is achieved. Digital Strategy for Europe

Cross-border digital identity and trust services are also rightly identified as a priority area. For Ukraine, integration into the European Digital Identity Framework can significantly expand the opportunities for citizens and businesses to access European administrative and commercial services, confirm qualifications, sign documents and carry out cross-border electronic transactions. At the same time, such integration requires a high level of security, reliable certification and protection of personal data [71]. In addition, it is necessary to combine digital integration with a European policy of technological resilience. In 2026, the EU further strengthened its emphasis on technological sovereignty, the development of its own semiconductor, cloud, AI and open-source solutions, as well as the security of digital supply chains [74, 75].

The integration of Ukraine into the European environment of artificial intelligence, data and cloud technologies should undoubtedly be defined as a strategic direction. As of 2025, Ukraine had not yet been brought into line with the AI Act, but had already developed a White Paper, an AI regulatory roadmap and a national strategy, which are considered by the Commission as a basis for further approximation [61]. The prospects of this direction are strengthened by the fact that the EU digital policy in 2026 is increasingly focused on the development of AI, secure cloud and data infrastructures, semiconductors and computing capacity [73, 74].

Thus, it is advisable to consider Ukraine's digital integration as an interconnected system of three components: security imperatives, risks, and strategic perspectives. Security imperatives determine the necessary conditions for integration; risks reflect vulnerabilities that may arise or intensify in the process of rapprochement; strategic perspectives characterize the directions in which digital integration is able to create long-term institutional and economic advantages. It is this logic that underlies the author's model of Ukraine's digital integration with the EU (Fig. 4.7), the main principle of which is to ensure secure and functionally compatible integration, in which each new level of interaction is accompanied by the necessary legal, institutional, technological, and personnel capabilities.

In general, Ukraine's digital integration into the European Union is simultaneously a process of regulatory convergence, technological modernization, market integration, and security transformation. Its effectiveness will be determined not by the number of formally implemented norms, but by the real compatibility of Ukrainian institutions, digital infrastructures, regulatory mechanisms, and protection standards with the relevant elements of the EU digital system. It is this compatibility that creates the prerequisites for the transition from individual formats of sectoral cooperation to Ukraine's sustainable participation in the European digital space.

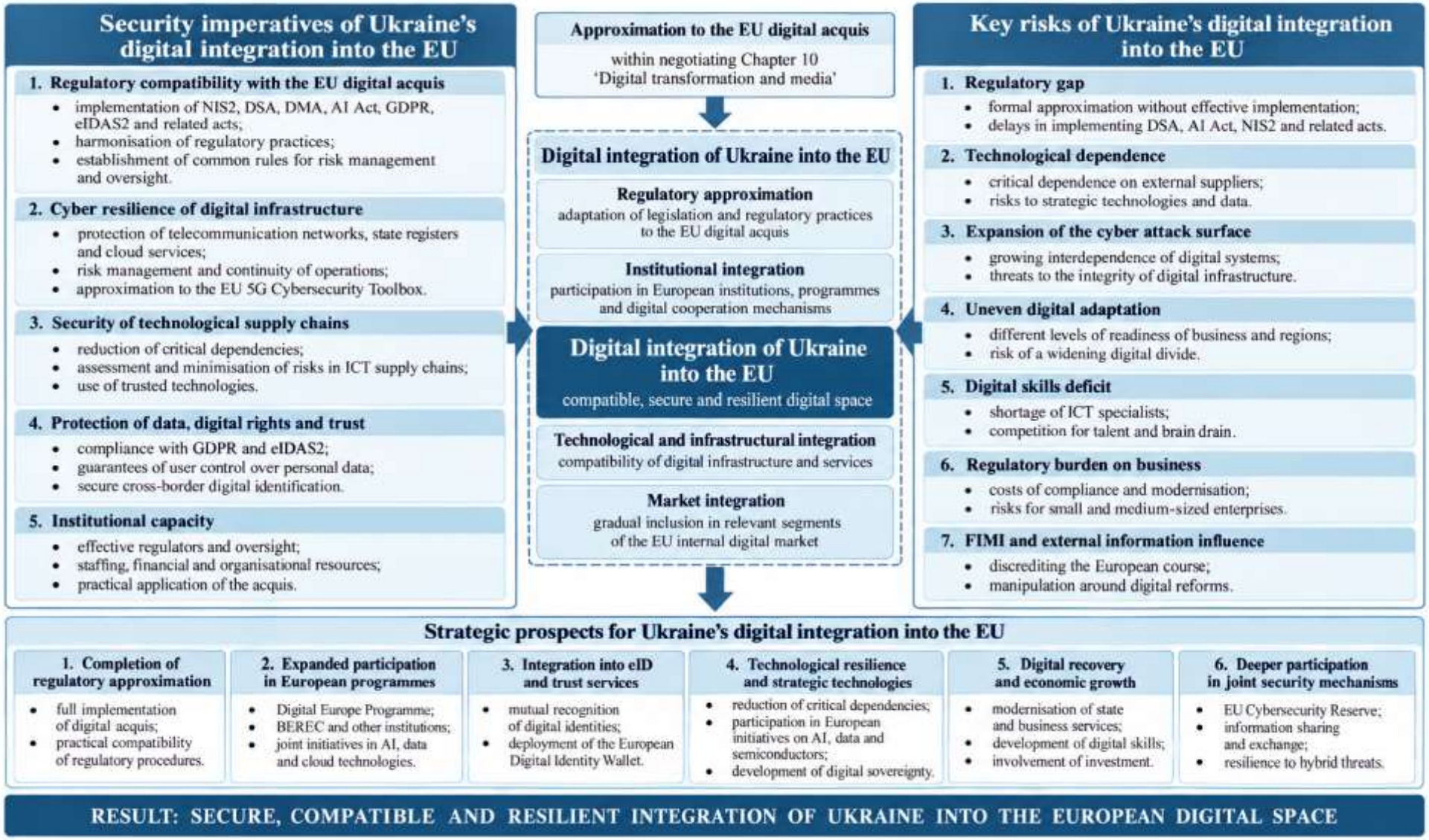


Fig. 4.7. Model of digital integration of Ukraine into the European Union: security imperatives, risks and strategic prospects

Source: developed based on [61, 68–82].

Thus, the study suggests that, in the current landscape, information and cybersecurity are increasingly transcending the boundaries of specific functional areas of state policy and assuming systemic importance for ensuring digital resilience. The European Union has established an extensive institutional-legal and institutional-organizational architecture that integrates strategic planning, legal regulation, coordination, monitoring, information sharing, crisis response, and capacity building. It is precisely the comprehensive nature of this model that enables it to adapt to the evolving nature of information and cyber threats while maintaining an adequate level of security for the digital environment.

For Ukraine, it is particularly significant that the transformation of information threats is occurring alongside the deepening of European integration. Russian information operations, FIMI, cyber threats, and other forms of hybrid influence are increasingly transnational in nature; they target not only individual states but also public trust in democratic institutions, societal resilience, support for Ukraine's European integration path, and the functioning of critical digital systems.

Under these circumstances, countering such threats requires not isolated national solutions, but rather deeper cooperation between Ukraine and European Union institutions, mechanisms, and platforms. The strategic partnership between Ukraine and the EU in the realm of cybersecurity is taking shape as a multi-level system encompassing political dialogue, regulatory alignment, institutional interaction, operational-technical cooperation, cyber capacity building, and cyber solidarity mechanisms. At the same time, the further development of this partnership should be linked not only to adapting to specific requirements of the European "acquis" but also to the gradual integration of Ukraine into joint mechanisms for prevention, detection, response, and recovery in the cybersecurity domain.

Simultaneously, Ukraine's digital integration into the European Union expands the scope of security cooperation. While it entails achieving regulatory, institutional, technological, and market compatibility, it also brings to the fore new risks associated with technological dependencies, an expanded cyber-attack surface, uneven digital adoption, skills shortages, and external information influence. Therefore, the security dimension must accompany every stage of integration into the European digital space.

Ultimately, Ukraine's place within the architecture of European digital resilience will be determined not merely by the degree of formal alignment with EU norms and standards, but primarily by its actual capacity to ensure their practical implementation, the compatibility of institutions and infrastructures, operational interoperability, and resilience against complex information and cyber threats. It is the combination of institutional alignment, joint response, technological interoperability, and security resilience that forms the strategic foundation for Ukraine's further integration into the European digital space.

References

1. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association*, 29(5), 818–835. URL: https://scibulcom.net/en/article/L8nV7It2dVTBPX09mzWB

2. European External Action Service. (2016). Shared vision, common action: A stronger Europe. A global strategy for the European Union's foreign and security policy. URL: https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

3. Onyshchenko, S., & Hlushko, A. (2022). Analytical dimension of cybersecurity of Ukraine in the conditions of growing challenges and threats. *Economics and Region*, 1(84), 13–20. https://doi.org/10.26906/EiR.2022.1(84).2540

4. Hlushko, AD (2020). Institutional and legal support for information security of the national economy. In The 18th International Conference "Information Technologies and Management 2020". ISMA University of Applied Sciences. URL: https://reposit.nupp.edu.ua/item/8388

5. Hlushko, A., & Herasymenko, M. (2025). Information security in Ukraine: Adaptation and implementation of European experience. In 100-th Economic and Legal Discussions. Series: Social and Human Sciences (pp. 3–4). URL: https://reposit.nupp.edu.ua/item/16731

6. European Commission. (2018). Tackling online disinformation: A European approach (COM (2018) 236 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

7. European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2018). Action plan against disinformation (JOIN (2018) 36 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0036

8. European Commission. (2020). EU Security Union Strategy (COM (2020) 605 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52020DC0605

9. European Commission. (2020). European democracy action plan (COM (2020) 790 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0790

10. European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2020). The EU's cybersecurity strategy for the digital decade (JOIN (2020) 18 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0018

11. European Commission. (2021). 2030 Digital Compass: The European way for the Digital Decade (COM (2021) 118 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0118

12. Council of the European Union. (2022). A strategic compass for security and defense: For a European Union that protects its citizens, values and interests and contributes to international peace and security. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

13. European Parliament, & Council of the European Union. (2022). Decision (EU) 2022/2481 of 14 December 2022 establishing the Digital Decade Policy Program 2030. *Official Journal of the European Union*, L 323, 4–26. URL: https://eur-lex.europa.eu/eli/dec/2022/2481/oj

14. European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2023). European economic security strategy (JOIN (2023) 20 final). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020

15. European Commission. (2025). European Democracy Shield. URL: https://commission.europa.eu/publications/european-democracy-shield-documents_en

16. European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

17. European Parliament, & Council of the European Union. (2016). Directive (EU) 2016/680 of 27 April 2016. *Official Journal of the European Union*, L 119, 89–131. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj

18. European Parliament, & Council of the European Union. (2018). Regulation (EU) 2018/1725 of 23 October 2018. *Official Journal of the European Union*, L 295, 39–98. URL: https://eur-lex.europa.eu/eli/reg/2018/1725/oj

19. European Parliament, & Council of the European Union. (2022). Regulation (EU) 2022/2065 of 19 October 2022 (Digital Services Act). *Official Journal of the European Union*, L 277, 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

20. European Commission. (2022). 2022 strengthened Code of Practice on Disinformation. Publications Office of the European Union. https://doi.org/10.2759/895080

21. European Commission. (2025). Code of Practice on Disinformation becomes a Code of Conduct under the Digital Services Act. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

22. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1083 of 11 April 2024 (European Media Freedom Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1083/oj

23. European Parliament, & Council of the European Union. (2018). Directive (EU) 2018/1808 of 14 November 2018 amending Directive 2010/13/EU on audiovisual media services. *Official Journal of the European Union*, L 303, 69–92. URL: https://eur-lex.europa.eu/eli/dir/2018/1808/oj

24. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/900 of 13 March 2024 on the transparency and targeting of political advertising. URL: https://eur-lex.europa.eu/eli/reg/2024/900/oj

25. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonized rules on artificial intelligence. URL: http://data.europa.eu/eli/reg/2024/1689/oj

26. Brogi, E., & Nenadić, I. (2026). The European Union's fight against online disinformation: Can safeguarding fundamental rights harm fundamental rights? In M. Senftleben, K. Irion, T. McGonagle, & J. Poort (Eds.), The Cambridge handbook of media law and policy in Europe (pp. 238–254). Cambridge University Press. https://doi.org/10.1017/9781009568159.016

27. European Parliament, & Council of the European Union. (2019). Regulation (EU) 2019/881 of 17 April 2019 (Cybersecurity Act). *Official Journal of the European Union*, L 151, 15–69. URL: http://data.europa.eu/eli/reg/2019/881/oj

28. European Parliament, & Council of the European Union. (2022). Directive (EU) 2022/2555 of 14 December 2022 (NIS 2 Directive). *Official Journal of the European Union*, L 333, 80–152. URL: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

29. European Parliament, & Council of the European Union. (2022). Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities. *Official Journal of the European Union*, L 333, 164–198. URL: http://data.europa.eu/eli/dir/2022/2557/oj

30. European Parliament, & Council of the European Union. (2023). Regulation (EU, Euratom) 2023/2841 of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: http://data.europa.eu/eli/reg/2023/2841/oj

31. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/2847 of 23 October 2024 (Cyber Resilience Act). URL: http://data.europa.eu/eli/reg/2024/2847/oj

32. European Parliament, & Council of the European Union. (2025). Regulation (EU) 2025/38 of 19 December 2024 (Cyber Solidarity Act). URL: http://data.europa.eu/eli/reg/2025/38/oj

33. European Parliament, & Council of the European Union. (2022). Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union, L 333, 1–79. URL: http://data.europa.eu/eli/reg/2022/2554/oj

34. European External Action Service. (2026). Information integrity and countering foreign information manipulation and interference (FIMI). URL: https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

35. Europol. (2026). European Cybercrime Center – EC3. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

36. European Commission. (2026). European Board for Digital Services. URL: https://digital-strategy.ec.europa.eu/en/policies/dsa-board

37. European Data Protection Supervisor. (2026). About the European Data Protection Supervisor. URL: https://www.edps.europa.eu/about-edps_en

38. European Commission. (2026). European Digital Media Observatory (EDMO). URL: https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

39. European Commission. (2026). European Center for Democratic Resilience. URL: https://commission.europa.eu/european-centre-democratic-resilience_en

40. Pylypchuk, R. V. (2011, updated 2024). Information War. In Encyclopedia of Modern Ukraine. Institute of Encyclopedic Research of the NAS of Ukraine. https://esu.com.ua/article-12460

41. Kharamurza, D. (2023). Information terrorism as a tool of hybrid warfare and a factor in the destruction of the media space. *Integrated Communications*, 2(16), 29–37. https://doi.org/10.28925/2524-2644.2023.163

42. Mytko, A. M., & Koltsova, I. I. (2018). Information terrorism as a tool for influencing information conformity in the global environment. *Political Life*, 2, 135–139. https://doi.org/10.31558/2519-2949.2018.2.22

43. Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2022). Russian propaganda on social media during the 2022 invasion of Ukraine. *arXiv*. https://doi.org/10.48550/arXiv.2211.04154

44. Onyshchenko, S., Maslii, O., & Hlushko, A. (2025). Digital and economic security of the state under global threats. In S. Dovgyi, E. Siemens, L. Globa, O. Kopiika, & O. Stryzhak (Eds.), Applied innovations in information and communication technology (Lecture Notes in Networks and Systems, Vol. 1338, pp. 580–602). Springer. https://doi.org/10.1007/978-3-031-89296-7_29

45. President of Ukraine. (2021). On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy": Decree of the President of Ukraine dated December 28, 2021 No. 685/2021. URL: https://zakon.rada.gov.ua/laws/show/68 5 /2021

46. European External Action Service. (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defense. Brussels: European External Action Service. URL: https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

47. European External Action Service. (2025). Report on EEAS activities to counter Foreign Information Manipulation and Interference (FIMI) in 2024. URL: https://www.eeas.europa.eu/sites/default/files/2025/documents/2024%20Report%20on%20EEAS%20Activities%20to%20Counter%20FIMI.pdf

48. Council of the European Union. (2024). Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States. 8 October 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/10/08/hybrid-threatsrussia-statement-by-the-high-representative-on-behalf-of-the-eu-on-russia-s-continued-hybrid-activity-against-the-eu-and-its-member-states/

49. Council of the European Union. (2024). Information manipulation in Russia's war of aggression against Ukraine: EU lists two individuals and one entity. 27 May 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-two-individuals-and-one-entity/

50. European External Action Service. (2026). 4th EEAS Report on Foreign Information Manipulation and Interference Threats. Brussels: EEAS. URL: https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web.pdf

51. European External Action Service & Center for Countering Disinformation. (2026). Russian FIMI targeting Ukraine's path towards EU membership. URL:

https://www.eeas.europa.eu/eeas/new-joint-report-exposes-desperate-russian-attempts-derail-ukraine%E2%80%99s-journey-towards-eu-membership_en

52. Council of the European Union. (2025). Russian hybrid threats: EU lists nine individuals and six entities responsible for destabilizing actions in the EU and Ukraine. 15 July 2025. URL: https://www.consilium.europa.eu/en/press/press-releases/2025/07/15/russian-hybrid-threats-eu-lists-nine-individuals-and-six-entities-responsible-for-destabilising-actions-in-the-eu-and-ukraine/

53. Onyshchenko, S., Zhyvylo, Y., Hlushko, A., & Bilko, S. (2024). Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, 5, 136–142. https://doi.org/10.33271/nvngu/2024-5/136

54. Savchuk, SO (2024). Challenges and Opportunities of Ukraine's Integration into the EU Cybersecurity System. Economics, Management and Administration, 2(108), 198–203. https://doi.org/10.26642/ema-2024-2(108)-198-203

55. European Commission. (2024, July 15). Ukraine: 3rd Cyber Dialogue with the European Union takes place in Brussels. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels

56. European External Action Service. (2025, October 16). EU and Ukraine deepen cooperation on cyber security at the 4th Cyber Dialogue. URL: https://www.eeas.europa.eu/delegations/ukraine/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue_en

57. European Union Agency for Cybersecurity. (2023, November 13). Enhanced EU-Ukraine cooperation in cybersecurity. URL: https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity

58. European Union Agency for Cybersecurity. (2025). ENISA International Strategy. URL: https://www.enisa.europa.eu/sites/default/files/2025-12/MB%20Decision%202025-21%20on%20adopting%20ENISA%20International%20Strategy%20with%20annex.pdf

59. European Commission. (2024). Proposal for a Council Implementing Decision on the approval of the assessment of the Ukraine Plan (COM(2024) 172 final). EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024PC0172

60. Council of the European Union. (2025). Council Implementing Decision (EU) 2025/1799. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025D1799

61. European Commission. (2025). Ukraine Report 2025. Directorate-General for Enlargement and Eastern Neighborhood. URL: https://enlargement.ec.europa.eu/ukraine-report-2025_en

62. Krainiuk, O., Yevseyev, S., Didenko, N., & Piksasov, M. (2025). Transformation of the regulatory and legal framework for cybersecurity in Ukraine: Analysis of compliance with the requirements of the NIS2 Directive and the Cybersecurity Act. *Territory of Security*, 1(3). https://doi.org/10.20998/3083-6298.2025.03.05

63. European Commission. (2026, June 11). EU-wide cyber exercise tests response to attacks on rail and maritime networks. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/eu-wide-cyber-exercise-tests-response-attacks-rail-and-maritime-networks

64. European External Action Service. (2024, December 19). A year of cyber support for Ukraine: The Tallinn Mechanism's milestone. URL: https://www.eeas.europa.eu/eeas/year-cyber-support-ukraine-tallinn-mechanism-milestone_en

65. European Commission. (2026, June 15). The EU provides cyber support to Ukraine against major attacks. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/eu-provides-cyber-support-ukraine-against-major-attacks

66. Axon, L., Saunders, J., Esteve-González, P., Carver, J., Dutton, W., Goldsmith, M., & Creese, S. (2025). Private-public initiatives for cybersecurity: The case of Ukraine. *Journal of Cyber Policy*, 10, 399–422. https://doi.org/10.1080/23738871.2025.2451256

67. Onyshchenko, S. V., & Hlushko, A. D. (2024). European paradigm of a secure digital world to increase economic sustainability. In Economic security: state, region, enterprise:

Proceedings of the VIII International Scientific and Practical Conference, May 16, 2024 (pp. 171–174). Yuriy Kondratyuk Poltava Polytechnic National University. URL: https://reposit.nupp.edu.ua/item/13411

68. European Commission. (2022, September 5). Solidarity with Ukraine: Digital Europe Program open to Ukraine to access calls for funding. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/solidarity-ukraine-digital-europe-programme-open-ukraine-access-calls-funding

69. European Commission. (2026, January 5). Roaming now fully operational in Ukraine. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/roaming-now-fully-operational-ukraine

70. European Commission. (2022, June 7). Commission Decision on Ukraine joining the work of BEREC. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/news/commission-decision-ukraine-joining-work-berec

71. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj

72. Council of the European Union. (2024). Council Implementing Decision (EU) 2024/1447 of 14 May 2024 on the approval of the assessment of the Ukraine Plan. Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/dec_impl/2024/1447/oj

73. European Commission. (2026). State of the Digital Decade 2026: Closing structural gaps and mobilizing investments for 2030 and beyond. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2026-closing-structural-gaps-and-mobilising-investments-2030-and-beyond

74. European Commission. (2026). Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy

75. NIS Cooperation Group. (2026). EU ICT Supply Chain Security Toolbox. European Commission. URL : https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security

76. Lola, YY, Mykhailenko, DH, Bolotna, OV, & Diachek, VV (2024). Ukraine's integration into the EU Digital Single Market. *The Problems of Economy*, 4(62), 64–70. https://doi.org/10.32983/2222-0712-2024-4-64-70

77. Vysochyn, I., & Zhuk, O. (2025). Ukraine's integration into the digital global space. *Foreign Trade: Economics, Finance, Law*, 138(1), 42–74. https://doi.org/10.31617/3.2025(138)03

78. Rabinovych, M. (2025). Wartime super-spillover? The perils and limits of a neofunctionalist approach to Ukraine's single market integration. Journal of European *Public Policy*, 32(12), 2886–2913. https://doi.org/10.1080/13501763.2024.2434693

79. Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European Union Digital Single Market governance. *Journal of Common Market Studies*, 62(1), 205–223. https://doi.org/10.1111/jcms.13488

80. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/792 of 29 February 2024 establishing the Ukraine Facility. *Official Journal of the European Union*. URL: https://eur-lex.europa.eu/eli/reg/2024/792/oj

81. European Commission. (2026). The Digital Europe Programme. Shaping Europe's Digital Future. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme

82. Iavorskyi, P., Taran, S., Shepotylo, O., & Hamaniuk, O. (2020). Ukraine's integration into the EU's Digital Single Market: Potential economic benefits. Ukrainian Center for European Policy. URL: https://ucep.org.ua/en/doslidzhennya/ukraines-integration-into-the-eu-digital-single-market.html

Appendix A

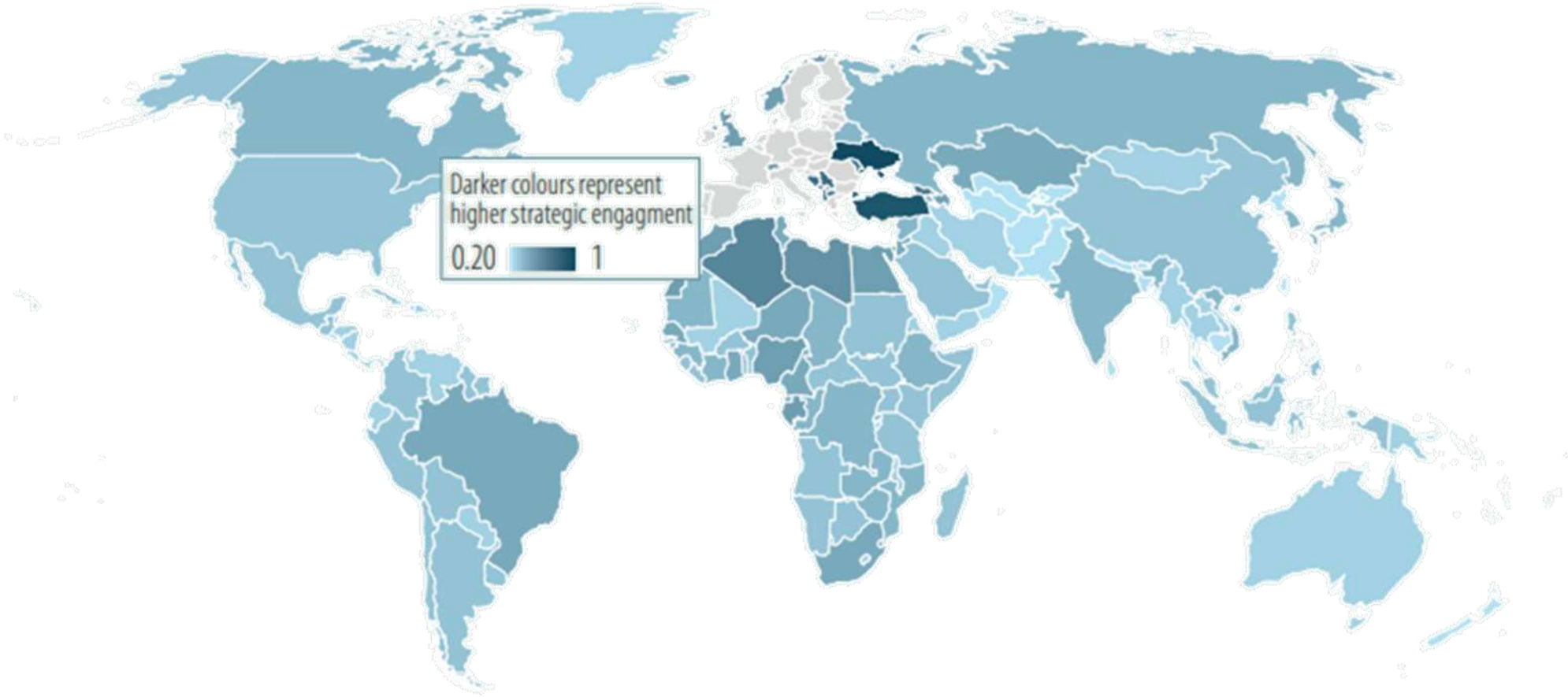


Fig. A.1. EU Strategic Engagement Index
Source: EIB Economics Department

Appendix B

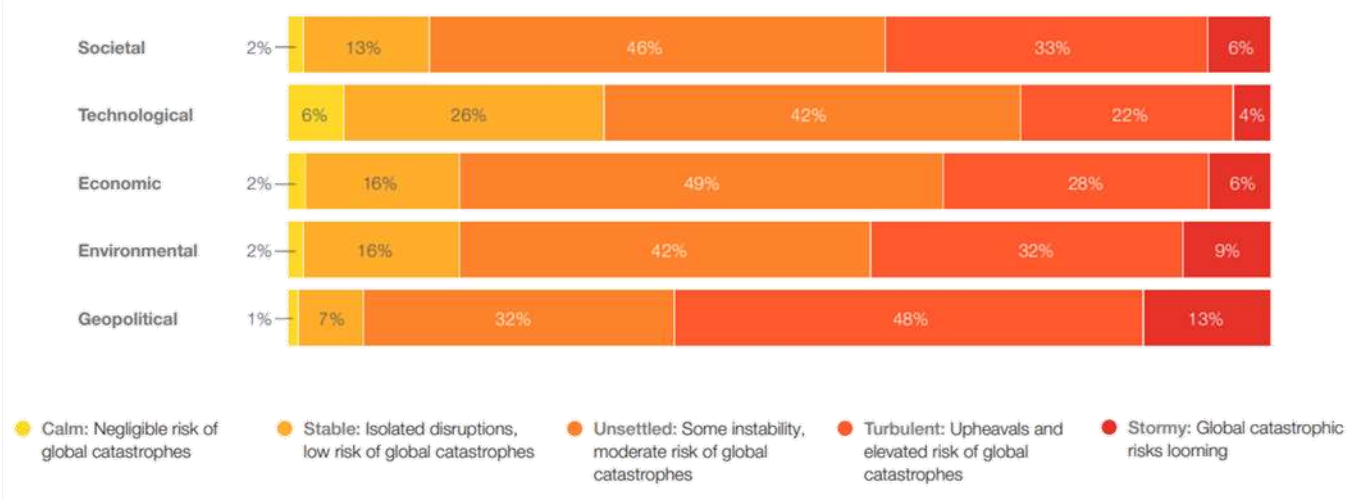


Fig. B.1. Short-term (2 years) outlook, by global risk category
Source: World Economic Forum Global Risks Perception Survey 2025-2026

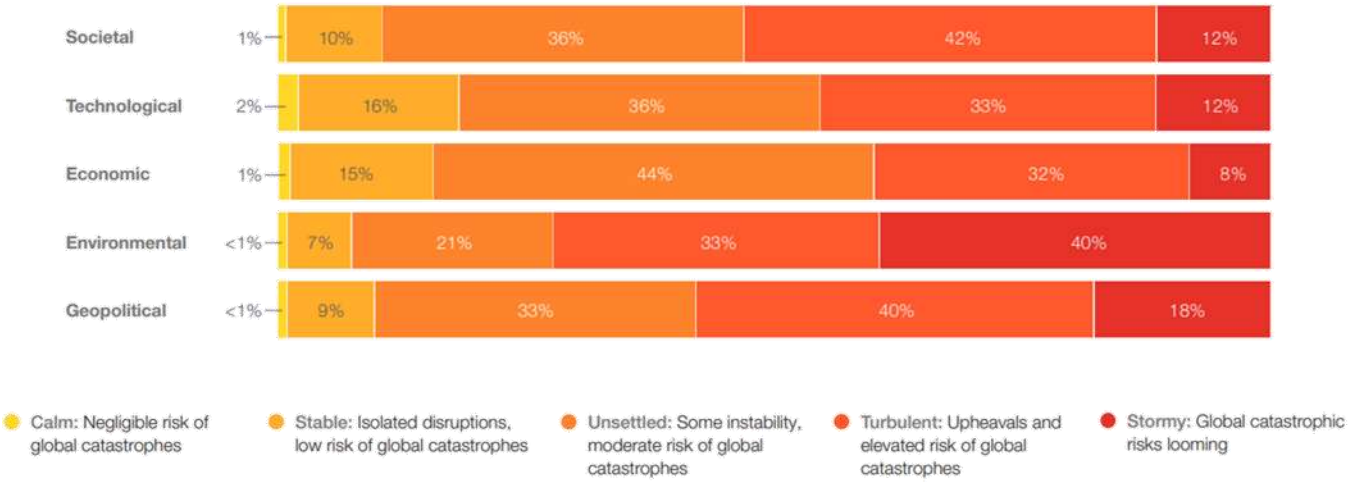


Fig. B.2. Long-term (10 years) outlook, by global risk category
Source: World Economic Forum Global Risks Perception Survey 2025-2026

Appendix C

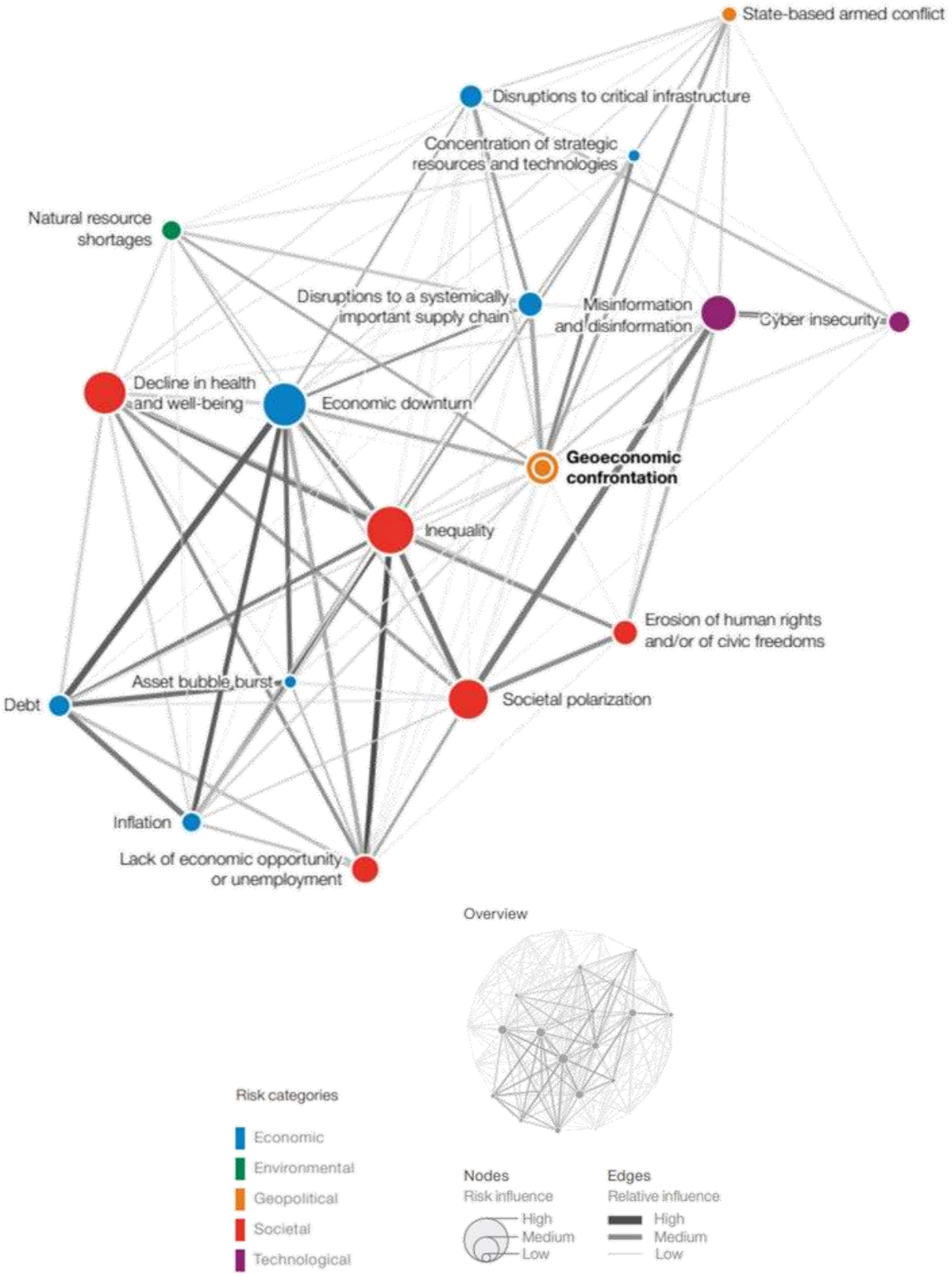


Fig. C.1. Global risks landscape: Geoeconomic confrontation

Source: World Economic Forum Global Risks Perception Survey 2025-2026

Executive Opinion Survey rank of national risks from the question "In your country, what are the top five risks that are most likely to pose the biggest threat to your country in the next two years?".

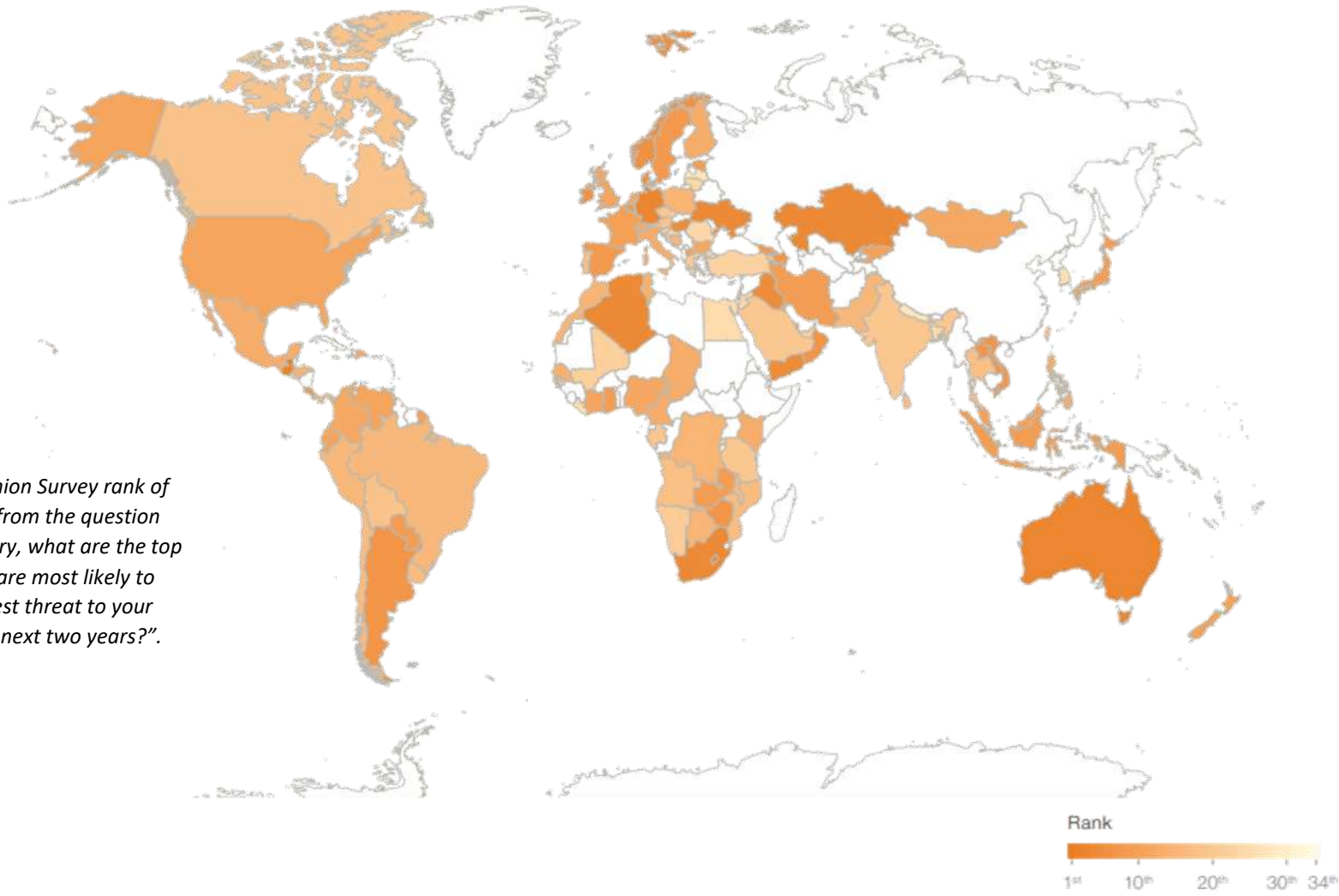


Fig. C.2. Executive perceptions of Disruptions to critical infrastructure, 2026-2028

Source: World Economic Forum Executive Opinion Survey 2025

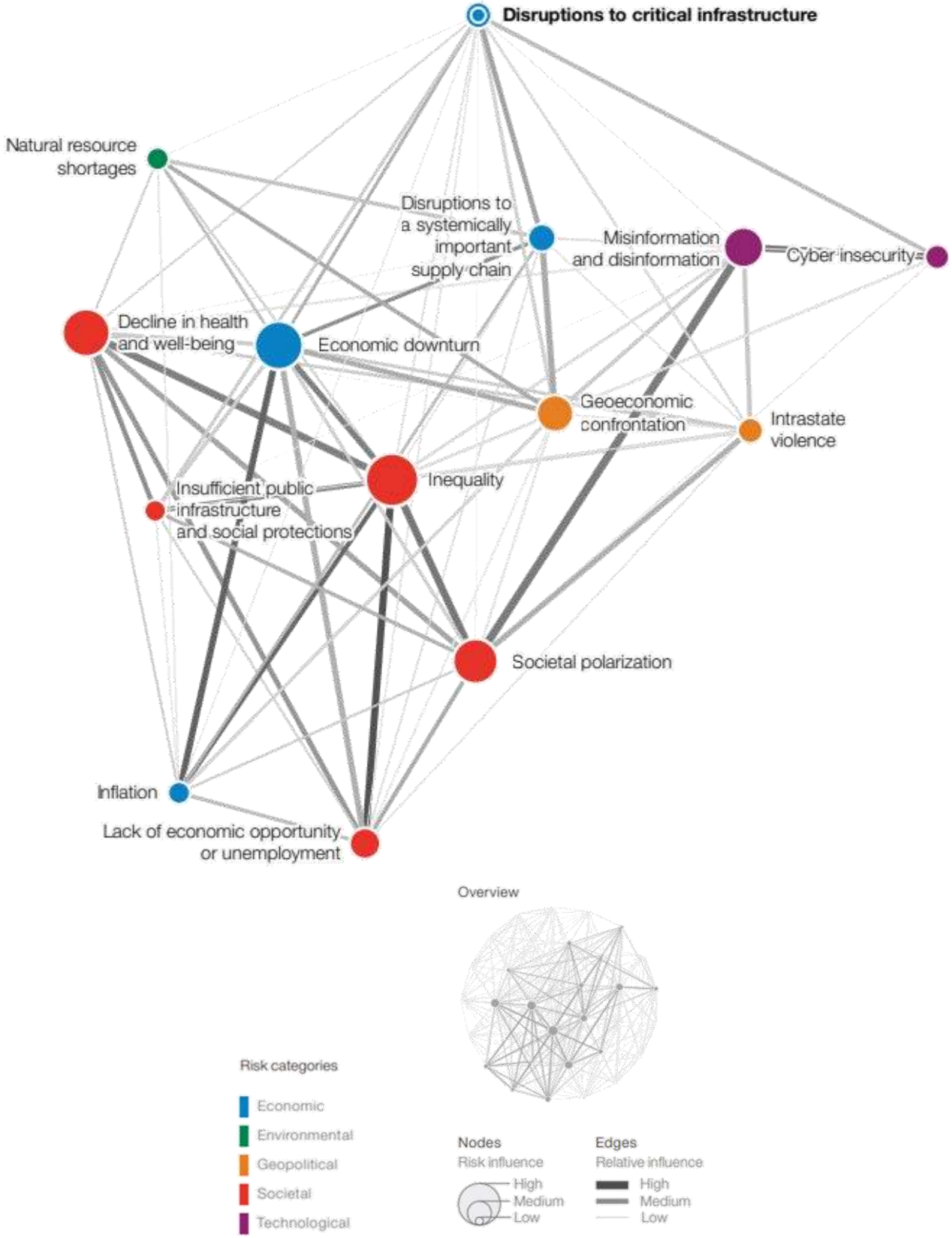


Fig. C.3. Global risks landscape: Disruptions to critical infrastructure

Source: World Economic Forum Global Risks Perception Survey 2025-2026

Appendix D

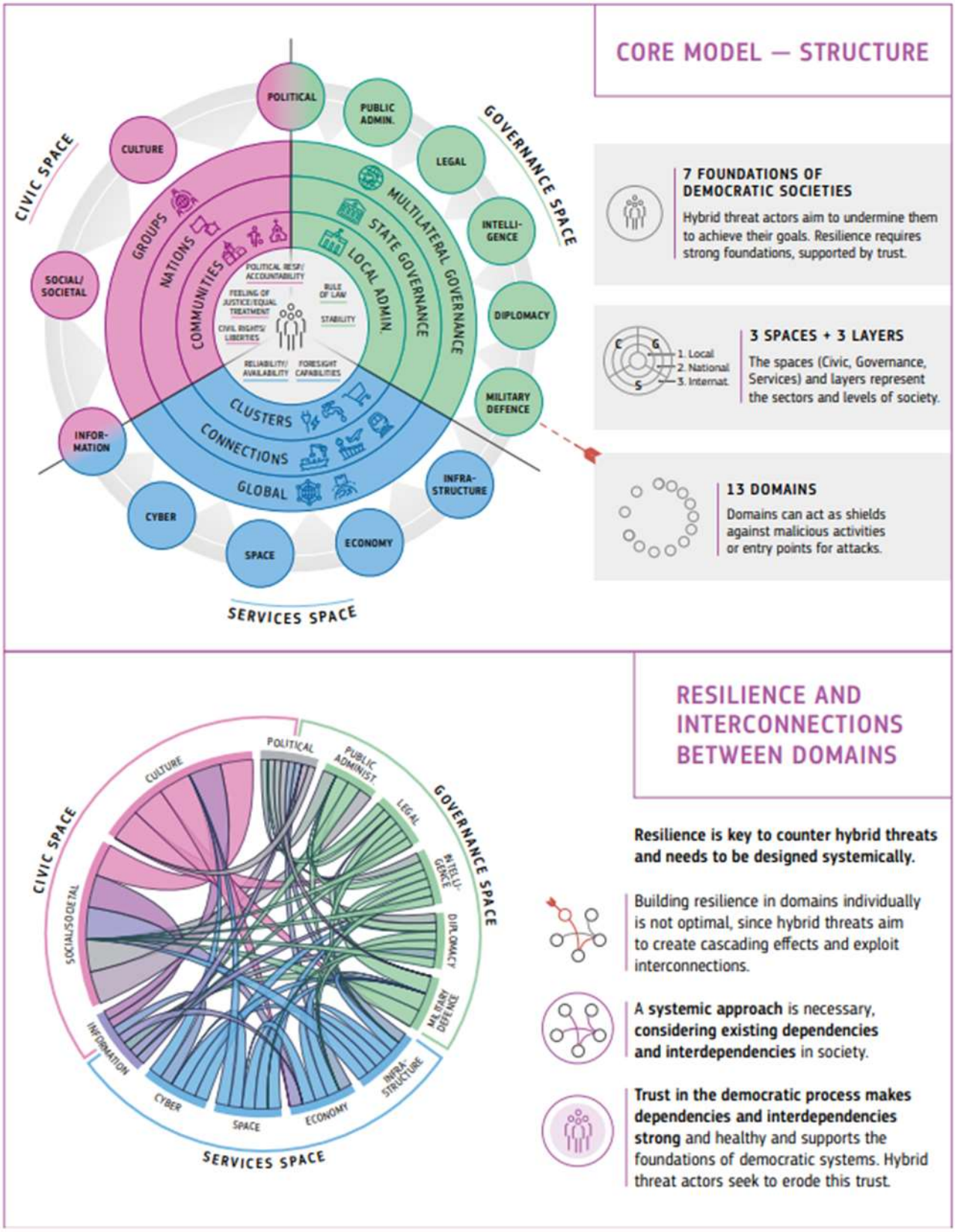


Fig. D.1. The comprehensive resilience ecosystem (CORE) model

Source: Joint Research Centre, European Commission, and the European Centre of Excellence for Countering Hybrid Threats

SCIENTIFIC EDITION

MONOGRAPH

ENVIRONMENTAL, ECONOMIC AND INFORMATION SECURITY OF UKRAINE IN COOPERATION WITH EU: CHALLENGES AND PERSPECTIVES

Authors:
Onyshchenko S., Maslii O., Hlushko A., Maksiuta N.

Monograph published in the author's edition
The monograph is included in International scientometric databases

Authorized for printing 15.10.2026.
Order No. MGE13-2026. Contracted price.

Published:
ScientificWorld -NetAkhatAV
Lußstr 13,
Karlsruhe, Germany

e-mail: editor@promonograph.org
https://de.promonograph.org

ISBN 978-3-98924-174-9

9 783989 241749