

EUROPEAN SECURITY ARCHITECTURE IN THE 21st CENTURY

Editors:
Anatolii ZADOIA
Svitlana FEDULOVA



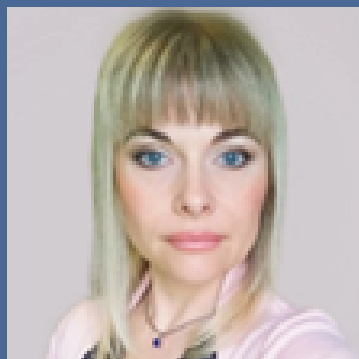


Anatolii ZADOIA,

Doctor of Sciences (Economic), Professor, Professor of the Department of Global Economics at Alfred Nobel University. Has many years of experience in teaching and research work at universities in Ukraine and Europe. Author of more than 300 scientific works. Honored Worker of Public Education of Ukraine.

Svitlana FEDULOVA,

Doctor of Sciences (Economic), Professor, Head of the Department of Global Economics at Alfred Nobel University. Experienced teacher and researcher. Leader and participant of many international Erasmus+ projects. Author of more than 190 scientific papers.



Alfred Nobel
University

duan.edu.ua

EUROPEAN SECURITY ARCHITECTURE IN THE 21st CENTURY

Editors:

Anatolii ZADOIA

Svitlana FEDULOVA

Dnipro, 2026

Reviewers:

O. I. Laiko,

*Doctor of Sciences (Economics), Full Professor, Deputy-director for
Scientific Work of the State Institution 'Institute of Market and
Economic&Ecological Research of the NAS of Ukraine';*

V. Ya. Shvets,

*Doctor of Sciences (Economics), Full Professor, Head of the Department of
Management of the National Technical University 'Dnipro Polytechnic';*

S. V. Filyppova,

*Doctor of Sciences (Economics), Full Professor, Director of the Institute of
Economics and Management of the Odesa Polytechnic National University*

E 26 European Security Architecture in the 21st Century:
Monograph. [Electronic Edition]. Edited by Prof. A. Zadoia, Prof.
S. Fedulova. Dnipro: Alfred Nobel University, 2026. 563 p.
<https://doi.org/10.32342/eurosec/9789664346266>

The monograph combines theoretical and methodological, analytical and applied levels of research. It offers a holistic vision of the architecture of global security, where economic, environmental, energy, digital and social dimensions are integrated. The focus is on Ukraine as an active subject in the formation of a new security order in Europe, based on the principles of sustainability, partnership, innovation and mutual responsibility.

The results of the study are interdisciplinary in nature and will be useful to all those interested in the prospects for building a new European security architecture.

ISBN 978-966-434-626-6



**Co-funded by
the European Union**

The monograph was prepared within the framework of the implementation of the international project 'Highlighting the New European Security Architecture in Teaching and Research', No. 101126795 – EuSANU – 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 the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

© A. Zadoia, S. Fedulova, 2026
© Alfred Nobel University, 2026

ISBN 978-966-434-626-6

Table of Content

<i>Preface</i>	6
<i>Introduction</i>	8
Section 1. General Principles for Building a New Global Security System	11
<i>Chapter 1.</i> Modern architecture of global security: which structural elements need to be replaced	12
<i>Chapter 2.</i> Global security in a world of change under the influence of development factors and emerging threats	30
<i>Chapter 3.</i> Geopolitical recession and the path to a new global security system	50
<i>Chapter 4.</i> Security of cross-border territories under the conditions of the Euroregional cooperation development	67
<i>Chapter 5.</i> Global business risks and directions for their minimization	90
<i>Chapter 6.</i> Strategic aspects of energy and environmental security management	106
Section 2. Dialectics of Global, Regional and National Security	126
<i>Chapter 7.</i> Global issues of the modern world and European security	127
<i>Chapter 8.</i> Security challenges of the 21st century: harmonization of global and national interests	155
<i>Chapter 9.</i> Formation of a sustainable development model of the state to ensure national security	173
<i>Chapter 10.</i> Coordinating security actions in Europe based on common perceptions of economic competition and logistics	199
<i>Chapter 11.</i> Ukraine's contribution to human resource security and reducing disparities in the European labour market	218
Section 3. Economic Security of Europe and its Components	232
<i>Chapter 12.</i> Economic security as an institutional prerequisite for the innovative development of society	233

<i>Chapter 13.</i> The European Union's Common Foreign and Security Policy (CFSP): challenges and prospects for Ukraine	248
<i>Chapter 14.</i> Formation of a regional policy of public administration cohesion with due regard to EU regulations: adaptation to security challenges and post-war recovery	262
<i>Chapter 15.</i> Europe's economic security in the era of artificial intelligence and digital transformation	280
<i>Chapter 16.</i> Intelligent systems for occupational safety supervision and management in European countries	295
<i>Chapter 17.</i> Corporate governance in the context of European security challenges	313
Section 4. European Security and Ukraine	330
<i>Chapter 18.</i> Ukraine as a key player in European security: geopolitical and economic aspects	331
<i>Chapter 19.</i> Competitiveness of corporate associations of enterprises in the system of Ukraine's cross-border integration into the EU	346
<i>Chapter 20.</i> European security and Ukraine: the role of international organizations in financial stability	361
<i>Chapter 21.</i> Investment case of post-war recovery of Ukraine: cross-border hydrogen clusters, near-shoring, innovation taxation	378
Section 5. Digital Transformation of Global Security	394
<i>Chapter 22.</i> The impact of digitalization on the competitiveness of Ukrainian businesses in the EU market: challenges and opportunities	395
<i>Chapter 23.</i> The impact of digitalization risks on the formation of the human resource potential of enterprises of the region and it's reflection in their development management strategies	419
<i>Chapter 24.</i> Digital management in ensuring the economic security of organizations under the dominance of Big Tech	437

<i>Chapter 25.</i> Environmental and digital transformation as instruments for strengthening global economic security: strategic objectives and outcomes of the European Union	456
Section 6. Integration of Ukraine into the European Economic and Political-Legal Space	475
<i>Chapter 26.</i> Methodological approaches to enhancing the effectiveness of integration processes within the EU economic and political-legal space	476
<i>Chapter 27.</i> The impact of European integration processes on the development of the judiciary in Ukraine	494
<i>Chapter 28.</i> The role of Ukraine in the transformation of the European security order: from partnership to full membership	513
<i>Chapter 29.</i> Transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU	537
<i>Contributors</i>	558

Preface

Modern geopolitical and geoeconomic processes testify to fundamental shifts in the world order, convincingly demonstrating the strengthening of security factors as one of the key ones that influence the formation of national political, legal and economic strategies. Vulnerabilities of the modern international legal order are provoked by inconsistent, and sometimes deliberate actions of countries that occupy leading positions in world trade, have significant potential in the military sphere and influential political power in relations with other states.

The military aggression against Ukraine, which continues to this day, sends a powerful signal to international organizations and supranational associations that international security safeguards are ineffective and, in this regard, issues of intensifying investment in defense technologies and deepening cooperation between countries in various areas of their common interests appear on the agenda of building a security architecture. This is especially important for strengthening military capabilities and increasing the effectiveness of financial and economic support for cooperation between the European Union and Ukraine on the basis of strategic forecasting and the formation of adaptive legal regulation.

The European Union recognizes Ukraine as part of the European security architecture, as proclaimed in the White Paper on European Defense – Readiness 2030. Measures capable of integrating the Ukrainian defense industry into the European Defense Technological and Industrial Base are recognized as priorities for strengthening the EU's defense capabilities.

This should be considered in the context of much broader European integration processes aimed at bringing the national legal system closer to the law of the European Union. Preservation of the fundamental values on which the European Union is founded simultaneously becomes the ideological basis for reforming the national mechanism of public administration, structural changes in the economy, and building civil society. The implementation of reforms in a stable and sustainable manner, based on the EU principles in the field of law-making, already today lays a solid foundation for preventing risks and minimizing their negative consequences.

A thorough assessment of the current transformations in the political, legal and economic systems of Ukraine, contained in this collective monograph, especially taking into account European integration priorities, forms a comprehensive vision of the further prospects for the integration of the Ukrainian state into the European security architecture.

Volodymyr USTYMENKO,
Corresponding Member of the NAS of Ukraine,
Corresponding Member of the NALS of Ukraine,
Doctor of Sciences (Law), Professor,
Honored Lawyer of Ukraine,
Director of the State Organization 'V. Mamutov
Institute of Economic and Legal Research
of National Academy of Sciences of Ukraine'

Introduction

In the 21st century, the global security system is undergoing a fundamental transformation, driven by a combination of classic geopolitical challenges and new threats, including hybrid conflicts, cyberattacks, energy shocks, pandemics, environmental crises, and structural deformations of the global economy. Classic notions of security as military-political stability no longer correspond to new realities. Today, security is becoming a multidimensional phenomenon that encompasses political, economic, social, informational, energy, environmental, and digital dimensions. At the same time, the system of international institutions created after World War II is increasingly less able to respond effectively to rapid global changes.

The monograph proposed by the authors is devoted to a comprehensive analysis of the modern architectonics of global security and the search for theoretical, methodological, and practical foundations for building its updated model. The purpose of the study is to substantiate a new system of global security in general and European security in particular, adapted to the conditions of a multipolar world, digital transformation and the growing interdependence of states, regions and corporations.

The first section reveals the general principles of building a new system of global security. It identifies key structural elements of the modern system that have lost their effectiveness and proposes conceptual directions for their renewal. The phenomenon of geopolitical recession is analyzed – a gradual decrease in the influence of traditional centers of power, which creates the prerequisites for the formation of a polycentric world. Special attention is paid to the issues of Euroregional cooperation, cross-border security, energy and environmental stability, as well as global business risks that shape new approaches to the management of international corporations.

The second section is devoted to the dialectics of the relationship between global, regional and national security. It analyzes the directions of harmonization of global and national interests in the context of security challenges of the 21st century, the role of European security as a component of the global order system, as well as the problems of forming a national model of sustainable development. A significant place is devoted to the topic of personnel security, reducing disparities in the EU labor market and Ukraine's contribution to the formation of European labor potential.

The third section reveals the economic security of Europe and its components, considering it as an institutional prerequisite for innovative

development and digital integration. The authors analyze the mechanisms of the EU Common Foreign and Security Policy (CFSP), the formation of a policy of public administration cohesion, adaptation to security challenges in the context of post-war recovery, as well as the impact of artificial intelligence, digitalization and corporate governance on the stability of the European economy.

The fourth section is of an applied nature and focuses on the role of Ukraine in the European security architecture. The potential of Ukraine as a key player in the European security system is considered, as well as its participation in the transformation of the labor market, cross-border integration, financial stability, and the development of innovative sectors of the economy. Particular attention is paid to investment cases of post-war recovery, in particular the creation of cross-border hydrogen clusters and the development of near-shoring production models, which are becoming a catalyst for Ukraine's integration into the European economic space.

The fifth chapter is devoted to the digital transformation of global security. It examines how digitalization, the development of artificial intelligence, Big Tech, and digital management systems are changing the risk structure, business competitiveness, and security strategies of states. The authors analyze the relationship between digitalization, environmental transformation, and the EU's global strategies in the field of sustainable development and economic security.

The sixth section outlines the directions of Ukraine's integration into the European economic and political and legal space, paying attention to methodological aspects of increasing the efficiency of integration processes, harmonization of legislation, development of the judiciary and transformation of the economic space of the de-occupied territories. It is through these processes that a new European security order is being formed, in which Ukraine is gradually moving from the status of a partner to a full participant.

Thus, the monograph combines theoretical and methodological, analytical and applied levels of research. It offers a holistic vision of the architecture of global security, where economic, environmental, energy, digital and social dimensions are integrated. The focus is on Ukraine as an active subject of the formation of a new security order in Europe, based on the principles of sustainability, partnership, innovation and mutual responsibility.

The author team represents scientists from various fields of research (economics, politics, law, technology, ecology, etc.) from all regions of Ukraine. This makes the research comprehensive, and its results interdisciplinary. Therefore, we are convinced that the monograph will be useful to all those who are interested in the problems of global and European security and the directions of its transformation in new geostrategic conditions.

The monograph was prepared within the framework of the implementation of the international project ‘Highlighting the New European Security Architecture in Teaching and Research’ No. 101126795 - EuSANU - ERASMUS-JMO-2023-HEI-TCH-RSCH and is the first in the planned cycle of publications dedicated to this topic.

Be always safe, dear readers!

*Anatolii Zadoia,
Doctor of Sciences (Economics), Ful Professor*

*Svitlana Fedulova,
Doctor of Sciences (Economics), Ful Professor*

Section 1
General Principles for Building a New
Global Security System

Chapter 1
***Modern architecture of global security: which structural
elements need to be replaced***
(A. Zadoia, O. Zadoia)

In the first third of the 21st century, the international security system is undergoing a profound transformation. The structures built after World War II are increasingly ill-suited to the realities of a polypolar (sometimes even unstructured), hybrid, and technologically complex world. Russia's war against Ukraine, the escalation of tensions between the United States and China, the erosion of arms control regimes, and the emergence of new security spheres (cyberspace, autonomous systems, space) all call into question the effectiveness of traditional security institutions. At the same time, the importance of economic, digital, and informational levers as instruments of coercion or protection is growing. In this context, there is an urgent need for a conceptual and practical rethinking of the global security architecture – its basic elements, hierarchy, role of global and regional actors, and the logic of interaction between them.

This chapter is devoted to a critical analysis of the contemporary global security architecture in order to identify its structural defects, justify the need for reform, and outline possible alternatives. The structure of the chapter includes three thematic blocks: historical context and evolution of security architecture; main defects and limitations of the current model; strategic directions for the modernization of global security through the installation of new structural elements.

1.1. The evolution of the global security system: political and economic dimensions

The global security system has undergone profound transformations since the mid-twentieth century. Geopolitical shifts, economic integration, and institutional development have been the main drivers of this transformation. This evolution reflects the complex interplay between political power dynamics and economic forces that continue to shape international relations today. Russia's full-scale war against Ukraine marks a turning point in world politics, illustrating the increasing attempts by authoritarian revisionists to undermine the rules-based international order established after World War II.

A survey conducted by experts at the Munich Security Conference in November 2024 among respondents from the G7 and BICS countries (BRICS, but excluding Russia) showed a general increase in the feeling of insecurity. Of course, the main source of danger is assessed differently in the countries studied. However, overall, after last year's decline in global risk perception, the Munich Security Index 2025 records a cumulative increase in 20 risk indicators, while ten indicators have decreased overall and two have remained stable [1]. The assessment of security prospects demonstrated by respondents is quite interesting. Only in China and India do respondents in the survey optimistically assess the possibilities of increasing security levels in the next 10 years (about 60% of respondents believe that in 10 years their country will be safer, while 11% and 18%, respectively, do not believe this). In the USA, South Africa and Brazil, the number of optimists and pessimists is almost the same. For European countries, the expectation of a worsening security situation in the next 10 years is characteristic. From 17% (Germany) to 24% (Great Britain) believe in an improvement in the level of security, while from 41% (Great Britain) to 52% (Germany) are pessimistic about the prospects. It is clear that European respondents consider Russia and Iran to be the main sources of danger. Interestingly, after the election of Donald Trump as US President, the perception of the risk posed by the US has increased sharply among other G7 countries, especially in Germany and Canada. This can be explained by fears of the start of tariff wars by the US. And as subsequent actions have shown, these fears have largely been justified. However, the most pessimistic respondents were from Japan: the number of those who expect the situation to worsen is 4 times greater than those who hope for an improvement (Table 1.1). For the Japanese, the main

sources of danger are North Korea and China. Also the close correlation between security expectations and belief in the growth of social wealth is indicative [1]. All of this is evidence that the existing security system is not trustworthy and requires significant reform.

Table 1.1

Respondents' opinions on whether their country will be safer in ten years, November 2024, in percentages*

Country	Agree	Don't know	Don't agree
China	60	30	11
India	58	24	18
UCA	35	33	32
SAR	35	30	36
Brazil	30	36	34
Canada	24	42	34
The UK	24	36	41
Italy	18	38	44
France	22	29	49
Germany	17	32	52
Japen	13	33	54

** Source: compiled by the authors based on [1]*

The post-World War II security architecture emerged from the ashes of global conflict and was built on four fundamental pillars: polarity, institutions, regimes, and customs. The international system shifted from pre-war multipolarity to a bipolar order dominated by the United States and the Soviet Union. This bipolarity was not spontaneous, but rather the result of changing power dynamics that began in the late 1930s and intensified during the war [2]. The architects of this new international order created institutions, processes, rules, and norms designed to facilitate collective problem-solving, deter protectionist impulses, and stabilize the global economy. This framework was based on both realist and normative principles – recognizing the importance of great powers and embedding liberal values in global governance [3]. As Zbigniew Brzezinski has noted, ‘strengthening global security is an essential component of national security’, recognizing that national and global security have become intrinsically linked [4].

As the expected global consensus gave way to Cold War tensions, these institutions served as points of unification against Soviet influence, while providing a basis for collective problem-solving and ensuring that the United States engaged in world politics in a way that promoted peace [3]. As a result,

multilateral sensitivity created patterns of cooperation that survived the Cold War itself.

International organizations were to play a crucial role in maintaining stability in the global security system. The United Nations, whose Security Council reflects the leadership of the great powers, became the central political institution of the postwar order. [3] NATO developed as a military alliance to protect Western interests, while the Organization for Security and Co-operation in Europe (OSCE) later became a platform for dialogue across the East-West divide.

On the economic front, the GATT system (1948–1995) and its successor, the World Trade Organization (1995–present), established a rules-based framework for international trade. The International Monetary Fund (IMF), the World Bank and the Bank for International Settlements (BIS) formed the institutional centre of the economic order, providing essential support in times of crisis. These institutions demonstrated their value, in particular, during financial emergencies such as the Latin American debt crisis, the Asian financial crisis of 1997 and the global financial crisis of 2007–2008.

The economic order that emerged was intended to guarantee the prosperity of its member states through a structured system of trade and investment. However, as the global landscape changes, these institutions are facing increasing pressure to reform.

Globalization, which has been developing since the 1980s, has fundamentally changed security issues at both the national and regional levels. At the economic level, globalization affects the security of nation states through the peculiarities of international transaction processes. Romanian researchers have identified globalization as a major factor in achieving national and regional security, suggesting that comprehensive security cannot be fully ensured without taking into account global economic integration [4].

The popularity of the liberal model of economic policy has had a significant impact on the reconceptualization of global risks, transforming traditional security threats into more complex, interconnected challenges. According to Rosenau, the late twentieth century witnessed a period of rapid change characterized by the transition from industrial to post-industrial orders focused on technology; the emergence of transnational problems affecting the global environment; the decline in the capacity of the state to resolve complex political and economic relations; and trends toward

decentralization [5]. These dynamics have continued to intensify in the twenty-first century.

However, the benefits of globalization are unevenly distributed. The implementation of models and theories of the liberal international order has led to significant inequality and slow growth in many regions, requiring reform if the overall order is to survive [3]. These economic imbalances can themselves become security threats when they fuel instability, extremism, or conflict.

A significant factor that changed the geostrategic situation was the transition from bipolarity to polypolarity [6]. After the collapse of the Soviet Union and the beginning of democratic and market transformations in the former Soviet republics, it seemed that the world had returned to a monocentric model, since the United States was the undisputed leader economically, politically, and technologically. However, the rapid growth of China's economy and its active foreign economic activity led to the fact that the economies of these countries became not just comparable: China is ahead of the United States in a number of indicators. The shadow of bipolarity has again "hung over" the world, but in a different composition and under different conditions. However, the 1990s of the 20th century and the 21st century, when there was no confrontation between the two centers and there was no need for countries to decide 'who you are for', played their role. A number of countries appeared that began to implement their leadership strategy, first at the regional level, and over time at the global level. Even when a new pair of leaders began to emerge, they did not take a clear side, but tried to pursue their own policies. Such countries include Japan, Turkey, India, Russia, etc. The world has become polycentric. Moreover, today it is perhaps even more accurate to use the characteristic 'disorderly polycentric' in relation to the global world order. In our opinion, a disorderly polycentric world is a concept of a modern international system in which there is no dominant center of power, and several states or blocs (the USA, China, the EU, India, Russia, Turkey, Brazil, etc.) exert influence simultaneously, without agreed rules of the game, an institutional arbiter, or a common vision of global order. This term describes the transition from a unipolar or bipolar world to a multiple world order in which:

- geopolitical centers of power compete with each other;
- international norms are fragmented or not recognized by all actors;
- the importance of regional unions, network structures is growing;

- the massive creation of ad hoc alliances as temporary coalitions or associations between states, organizations or other subjects of international relations to solve a specific problem or achieve a single goal (for example, the Global Coalition against ISIS, the Ramstein Coalition, the Crimean Platform, AUKUS, etc.);

- there is excessive conflict, contradictory strategies, and a lack of mechanisms for coordinating interests.

As Richard Haas notes, this is a “world without a center” in which power is distributed and institutions do not keep up with changes [7]. Such a model creates instability, increases the risk of conflict and complicates the development of collective solutions to global challenges (climate, war, technology, pandemics). Traditional security institutions created for a bipolar world are not able to work effectively in such conditions. Another factor destabilizing the existing architecture of global security are financial and political crises, which have repeatedly demonstrated their ability to undermine security at many levels. Recent studies provide compelling evidence that conflicts and political instability are associated with a higher probability of systemic banking crises, with the chances of a banking crisis being 2.5 times higher in countries affected by conflict. Furthermore, conflict duration is positively correlated with the probability of a crisis: the probability of experiencing a banking crisis reaches 25% if the conflict lasts ten years, compared to 16.4% for two-year conflicts [8].

Conflicts and political instability in one country can have a negative impact on the banking systems of neighboring countries. The main channel of transmission is fiscal crises that emerge after periods of conflict or political instability. This relationship between political stability and financial security highlights the complex relationship between different dimensions of the global security environment.

The evolution of the global security system reflects the ongoing tension between great power politics and institutional cooperation, between economic integration and national sovereignty. Although the post-war order has created unprecedented prosperity and stability for many countries, it faces serious challenges from populist movements, rising inequality, and renewed great power competition.

However, the most serious threat to the international order may be internal, not external. If Western and global populations continue to lose faith in the political and economic values and systems that are central to the order, it risks being “emptied from within” and losing its influence [3]. The Munich

Security Conference recognized that, in addition to undermining international law and human rights, the return to power politics challenges the multilateral cooperation urgently needed to address global challenges such as climate change and health emergencies [1]. The global security system must evolve towards more equitable multilateral governance, while preserving the core institutions and norms that have underpinned decades of relative peace and prosperity. This evolution will determine whether the system can effectively confront the security challenges of the 21st century or whether it will give way to a fundamentally different global order.

1.2. Design defects: what needs to be changed

The consistent application of principles inherited from the Cold War order has created a number of constructive limitations in the modern architecture of global security. These shortcomings not only undermine the effectiveness of key institutions, but also reduce the legitimacy of the world order in the eyes of most countries of the Global South. Table 1.2 lists the main elements of the classical global security architecture, highlighting their functions and identifying those weaknesses that have become particularly evident in the new geostrategic realities. Let us try to analyze them in more detail and prepare the basis for the subsequent justification of proposals for restructuring.

Table 1.2

Key elements of a classic global security architecture *

Element	Function	Weakness today
UN Security Council	International sanctions, peacekeeping	Veto blocking, unrepresentativeness
NATO, CFE, Open Skies Treaty	Control over conventional forces	Termination, security dilemma in Europe
Wassenaar Arrangement	Technology export control	Does not regulate cyberweapons and autonomous systems
WTO, global agreements	Trade regulation	Insufficient protection against political coercion, inability to resist increasing protectionist tendencies

** Source: compiled by the authors*

After Russia launched a full-scale war against Ukraine, the United Nations and its Security Council have been particularly criticized, demonstrating their absolute inability to influence the aggressor. Due to structural shortcomings, the Security Council is unable to make a decision against one of its permanent members, and the UN General Assembly can adopt two resolutions at the same meeting that contradict each other, as was the case, in particular, on the third anniversary of the full-scale war in Ukraine.

And this is not surprising. After all, the United Nations, established in 1945, reflects the geopolitical situation of the post-war world, and not the realities of the 21st century. This is especially true of the UN Security Council (UNSC), where the five permanent members (P5) – the United States, Great Britain, France, Russia, China – have the right of veto. Paradoxically, the world is still trying to solve security problems based on the principles that were implemented 200 years ago in the model of the first European international security model, created after the Napoleonic Wars and built on the principle of “the winner takes all” [9]. Meanwhile, large regional states such as India, Brazil, Nigeria, Japan or South Africa are deprived of the right of permanent representation. This asymmetry creates a sense of inequality and causes growing dissatisfaction, especially among the countries of the Global South. As Weiss notes, the structure of the UNSC is outdated and does not correspond to the principles of legitimate global governance [10]. Recognizing this, many states are calling for the expansion of the Security Council and a review of the veto mechanism, which often blocks even basic decisions in the security sphere.

Technological progress in recent years has significantly expanded the areas of threats to global and national security. However, the newest areas of potential conflict – cyberspace and outer space – remain largely unregulated at the global level. Back in 2001, the Budapest Convention on Cybercrime was adopted [11]. It was the first international treaty aimed at combating cybercrime and ensuring the security of electronic evidence. Compliance with the Convention provides a basis for harmonizing national legislation, promoting international cooperation and establishing procedures for investigating cybercrime. The Convention covers a variety of cybercrime offences, including copyright infringement, computer fraud, child pornography and breaches of network security. However, emerging threats such as autonomous cyberweapons, deepfake technologies or attacks on critical infrastructure remain outside the scope of current international law.

Outer space is also regulated to a limited extent – the Outer Space Treaty of 1967 prohibits the deployment of weapons of mass destruction, but does not provide answers to new challenges: the deployment of satellite intelligence systems, the privatization of space, military platforms in orbit. As modern researchers note, the legal vacuum in rapidly militarizing areas creates the risk of uncontrolled escalation [13]. At the same time, even the system of control over conventional arms, created during the Cold War, has lost its stability and effectiveness. The Treaty on Conventional Armed Forces in Europe (CFE) [14], the Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles (INF) [15], as well as the Open Skies Treaty [16] have effectively ceased to operate due to the withdrawal of the USA, Russia and other parties from them. This has led to instability in Europe unprecedented since the 1980s, especially against the backdrop of the Russian–Ukrainian war. Recently, many European countries, including Ukraine, have decided to withdraw from the Ottawa Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines [17], motivating such actions with the need to resist Russian aggression. As William Lippert notes, ‘it is necessary to create new agreements that take into account both conventional and high-precision weapons, as well as emerging technologies, in order to stop the arms race’ [18]. Such an architecture should include new rules of transparency, joint monitoring and restrictions on the use of autonomous systems.

Another fundamental paradigm of the post-war architecture of the international security situation – multilateral diplomacy (multilateralism) does not stand the test of modern conditions and is becoming increasingly fragmented. Formal international institutions, in particular the UN, quite often become an arena of confrontation between great powers, rather than cooperation. In parallel, the role of mini-lateral formats is growing: BRICS, G7, G20, AUKUS, QUAD, etc. Such formats often have greater flexibility and ability to act, but contribute to the fragmentation of the general global order. This can lead to ‘selective multilateralism’, where states choose only formats that are beneficial to themselves, avoiding joint obligations [19]. As a result, trust between countries deteriorates and the ability to respond to global crises decreases. Moreover, even within such fragmented associations, the problem of adopting a joint declaration that would meet the interests of all participants increasingly arises. In general, the results of the conducted studies of the constructive elements of the architecture of international security are presented in Table 1.3.

Table 1.3

Major design flaws in current security architecture *

Problem	Consequences
UNSC unrepresentativeness	States with large resources do not have permanent status
Unjustified veto rights	Delayed decisions, inequality in access to sanctions and peacekeeping
Lack of cyber and space regulations	Threat to the autonomy of systems from private and public cyberbots
Fracturing multilateralism	The spread of mini lateralism undermines the centralized scope of action of the UN and other international organizations

** Source: compiled by the authors*

Thus, the architecture of global security is in deep crisis not only due to external challenges (wars, pandemics, climate) but also due to internal structural defects: unrepresentativeness, normative stagnation, loss of arms control, and institutional fragmentation. All of these factors require not cosmetic changes, but a profound modernization of the foundations of the global order.

1.3. New constructive elements: alternatives and reform

The modern architecture of global security requires not only the repair of existing institutions, but also the introduction of new constructive elements that correspond to the realities of the 21st century. These elements should combine the principles of efficiency, inclusiveness, legal order and technological adaptability. Let us highlight just a few key areas of reform.

First of all, the United Nations and the UN Security Council need reform. Numerous proposals for reforming the Security Council can be grouped into three groups: expanding the total number of members; increasing the number of permanent members; limiting the range of issues on which the right of veto can be applied [20] (Fig. 1.1).

The proposal to increase the total number of members of the Security Council is not uncontested. On the one hand, this would indeed expand representation in the main institution that is supposed to be concerned with global security. In this case, the interests of different countries and regions of the world would be more fully represented and, perhaps, more reasoned

decisions would be made. On the other hand, any increase in the number of members would make the structure less flexible and more bureaucratic. This could negatively affect the effectiveness of this institution in a dynamically changing environment.

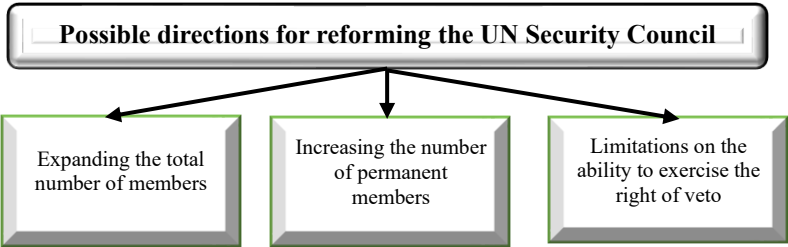


Fig.1.1. Possible directions for reforming the UN Security Council

The proposal to increase the total number of members of the Security Council is not uncontested. On the one hand, this would indeed expand representation in the main institution that is supposed to be concerned with global security. In this case, the interests of different countries and regions of the world would be more fully represented and, perhaps, more reasoned decisions would be made. On the other hand, any increase in the number of members would make the structure less flexible and more bureaucratic. This could negatively affect the effectiveness of this institution in a dynamically changing environment.

The UN Security Council, despite its status as the highest body on peace and security issues, is increasingly losing legitimacy due to unequal representation and the political paralysis caused by the veto. Well-known conflicts – from Syria to Ukraine – have shown that the veto often blocks decisions that have the support of the overwhelming majority of UN members. In response, it is proposed to create a new category of ‘semi-permanent’ or ‘rotating-permanent’ members, which could include India, Brazil, Nigeria, Japan and Germany – countries of significant regional and global importance. There are numerous proposals for special representation of Muslim countries. At the same time, the question of revising or limiting the veto power is being raised. One model is the introduction of a ‘retroactive veto’ or ‘retroactive approval’ mechanism – decisions that could be revised after their implementation in an emergency. The retroactive (retrospective)

veto mechanism was proposed as part of an initiative by the governments of France and Mexico, and also supported by the countries of the ‘Accountability, Coherence and Transparency’ group (ACT-Group) – as a voluntary norm prohibiting the use of the veto power in cases of genocide, war crimes and crimes against humanity. This concept is known as Responsibility Not to Veto (RN2V). In 2013, France and Mexico organized a ministerial meeting on this issue at the UN General Assembly, calling on member states to ‘refrain from using the veto in situations involving genocide, crimes against humanity, war crimes and ethnic cleansing’ [21]. In addition, the ACT Group, which included almost 30 states, actively recommended the creation of a formal code of conduct for permanent members that would limit the use of the veto in cases of mass crimes and provide for public justification of the decision. Unfortunately, however, this initiative was supported by only one permanent member of the Security Council, the United Kingdom. Therefore, the retrospective veto remains a voluntary political mechanism, but is not written into the UN Charter itself. It remains a political, not a legal, norm, and there is virtually no chance that this composition of the Security Council will agree to anything else.

Security is not just about politics and diplomacy. It is also about economics and big spending. The next step in rebuilding the security architecture could therefore be the creation of a specialized financial institution: the Defense–Security–Resilience Bank (DSR Bank). This ambitious idea, promoted by analysts at the Atlantic Council and the Financial Times, is to create a bank that issues AAA bonds to finance defense, cybersecurity, and resilience investments, primarily in countries that do not have access to long-term credit [22]. This bank could become the foundation for a global security supply system – similar to the role of the World Bank in the reconstruction of post-war Europe. Its functions could include: (1) guaranteeing arms supply chains; (2) lending to defense technology developers; (3) financing the modernization of armies of countries in the Global South; (4) deploying rapid response funds. This approach forms a new architecture of resilience finance, reducing dependence on national budgets and the political will of individual states [23, 24].

As already noted, modern conflicts are increasingly cyber-physical in nature. Attacks on infrastructure, control systems, deepfake communications and autonomous combat drones pose an existential threat. Despite this, international law remains fragmented. The only global agreement discussed

above – the 2001 Budapest Convention – does not cover the latest forms of threats and does not contain sanctions or enforcement mechanisms.

In this regard, there are increasing calls for a new Global Cyber Convention, which would regulate acceptable practices, prohibit the use of autonomous weapons without human control, and contain provisions on monitoring and sanctions [25].

In the space sector, it has been proposed to introduce a “Code of Conduct” for behavior in orbit, regulating the placement of weapons, space debris, and rules for approaching satellites of other states. Such a code is already being developed within the EU and is proposed for discussion in the UN General Assembly. An important role in this process should be played by the autonomous institute of the United Nations – the United Nations Institute for Disarmament Research (UNIDIR). Its mission is to promote dialogue and the development and implementation of innovative ideas to counter disinformation and international security, especially in the areas of arms control and non-standard threats. The institute works to create research, analytics, and practical recommendations for states, international organizations, the academic community, and civil society. Among its initiatives that have already been partially implemented or continue to be implemented, it is worth highlighting:

- launch of leadership conferences on space security (OS24, OS25);
- development of digital tools (development and unification of terminology in the field of space security to avoid misunderstandings between participants in discussions (Portal, Lexicon);
- inclusion of a wide international community through the Expert Network to discuss space security issues and support an inclusive dialogue taking into account the position of the Global South [26].

However, despite the fact that UNIDIR is the most authoritative institute in the field of disarmament and space security research, it cannot work effectively for several reasons. First, its decisions are purely advisory in nature. UNIDIR does not have the authority to make any decisions that would be binding. Second, its activities are financed only by voluntary contributions from countries. Limited and poorly predictable funding does not allow for strategic planning or the implementation of important monitoring activities. Third, the Institute has a rather limited influence on UN member states. The largest space powers (USA, China, Russia) due to conflicts of interest quite often simply ignore UNIDIR recommendations.

Possible ways to solve the listed problems could be to provide UNIDIR with stable funding from the UN and involve it in official events with a special mandate. It is also important to overcome the “elite” limitation, when only a limited number of diplomats and politicians participate in UNIDIR events. Through digitalization, the Institute’s research results and conclusions should be accessible to the general public, which will allow shaping public opinion and influencing political decisions.

Another key element of the European (and global) security architecture is arms control, which essentially collapsed during 2010–2022. The lack of transparency regarding the movement of forces, the buildup of strike weapons, the lack of communication channels during incidents – all this leads to an increase in the likelihood of an unintentional conflict. Experts from the Global Governance Institute and SIPRI propose creating a new version of the Treaty on Conventional Armed Forces in Europe (CFE II), which would include new types of weapons, flank agreements (arrangements on movement restrictions in border regions), digital monitoring systems based on AI and mandatory ‘transparent’ inspections [18].

It is also important to restore confidence-building measures (CBMs), including training alerts, hotlines between headquarters, data exchanges on procurement, and the creation of buffer zones. All of this was already partially implemented within the OSCE by the 2010s and can be updated in a new digital form [27]. In today's polycentric world, monolithic structures such as the UN are increasingly unable to respond quickly. In response, mini-lateral coalitions, which unite 3–5 countries around a specific task or regional challenge, are gaining popularity. Today, there are already dozens of such associations, including Ukraine. Most often, such associations are not formalized, without certain legal attributes (for example, ‘Rammstein’, ‘Crimean Platform’, ‘Czech Initiative’, etc.). These alliances can act flexibly, quickly, and technologically adaptively. Some authors propose developing a hybrid model in which minilateral initiatives operate within the framework of the general principles of the UN and the Vienna Convention, but with their own operational autonomy [28].

The analyzed approaches demonstrate that the security architecture of the 21st century should not be a simple restoration of the past, but an innovative attempt to reconcile technological realities, regional interests and the need for global legitimacy. Institutional reform, the creation of new financial and technological instruments, the introduction of regulatory

regimes for new security spheres – all this is a necessary condition for building a truly viable international order.

Thus, the existing global security architecture is a product of the past, but today is less suitable for maintaining stability in the face of political uncertainty, technological risks and climate shocks. Constructive elements such as veto rights, incomplete representation, lack of cyber control and an outdated arms-control system do not meet current needs. The proposed new constructive solutions provide flexibility, legitimacy, and the ability to respond promptly and collectively. This will allow us to move from an outdated model of world order to an adaptive, multi-level, and democratized architecture of global security that is capable of providing an adequate response to the challenges of the 21st century.

References

1. Munich Security Index 2025. Available at: https://securityconference.org/assets/02_Dokumente/01_Publikationen/2025/MSR_2025/Kapitel/MSR_2025_Munich_Security_Index.pdf
2. Bingöl, O. (2022). Transformation of international security architecture in 21st century and the challenges for Turkey. New world architecture of economy and security. PP. 447–463. Available at: https://tasam.org/Files/Icerik/File/yeni_dunya_ekonomi_ve_guvenlik_mim_arişi_IGK2019_5-448-464_pdf_e96a29a2-3c5f-4025-ae15-3c7f639afe0c.pdf
3. Mazarr, M. J. (2018). Summary of the building a sustainable international order project. 32 p. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2397/RAND_RR2397.pdf
4. Prunau, N. F. (2019). The influences of globalization on national security of states. EIRP Proceedings. Vol. 14 No. 1. Available at: <https://proceedings.univ-danubius.ro/index.php/eirp/article/view/1954/2356>
5. Mitrovic, M. (2019). Influence of global security environment on collective security and defence science. Security and Defence Quarterly. Vol. 24. No. 2. PP. 5–20. Available at: <https://securityanddefence.pl/pdf-106088-40434?filename=40434.pdf>
6. Kholod, B., Zadoia, A. Zadoia, O. (2020). Polycentrism of the modern world: a methodology for discovering world leaders. Naukovyi Visnyk

Natsionalnoho Hirnychoho Universytetu, No. 3, pp.171–176.
<https://doi.org/10.33271/nvngu/2020-3/1716>

7. Haass, R. (2020) The world: a brief introduction. New York: Penguin.
400 p. <https://doi.org/10.1093/ia/iab166>

8. Ali Compaoré, Mr. Montfort Mlachila, Rasmané Ouedraogo, Sandrine Sourouema (2020). The impact of conflict and political instability on banking crises in developing countries. International Monetary Fund. Vol. 2020. Issue 41. 40 p. Available at:
<https://www.elibrary.imf.org/view/journals/001/2020/041/article-A001-en.xml>

9. Zadoia, A. (2023). Stages of formation of modern European collective security. Трансформація економічних систем та інститутів у нових геостратегічних реаліях: Матеріали XXXV Міжнародної науково-практичної конференції молодих вчених і студентів, Дніпро, 27–28 листопада 2023 р. [Електронне видання]. Дніпро: Університет імені Альфреда Нобеля, с.109–115. Available at:
<https://ir.duan.edu.ua/handle/123456789/3909>

10. Weiss, T. G. (2016). What's Wrong with the United Nations and How to Fix It. Polity Press.

11. Council of Europe. Convention on Cybercrime (ETS No. 185). Available at: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>

12. Договір про принципи діяльності держав по дослідженню і використанню космічного простору, включаючи Місяць та інші небесні тіла. Available at: https://zakon.rada.gov.ua/laws/show/995_480#Text

13. Roscini, M. (2023). Cyber Operations and the Use of Force in International Law. Oxford University Press. 336 p.

14. Договір про звичайні збройні сили в Європі. Available at: https://zakon.rada.gov.ua/laws/show/994_314#Text

15. Arms Control Association. The Intermediate-Range Nuclear Forces (INF) Treaty at a Glance. Available at: <https://www.armscontrol.org/factsheets/intermediate-range-nuclear-forces-inf-treaty-glance>

16. Arms Control Association. The Open Skies Treaty at a Glance. Available at: <https://www.armscontrol.org/factsheets/openskies>

17. Україна виходить з Конвенції про заборону протипіхотних мін – Рада ухвалила закон. Available at: <https://www.ukrinform.ua/rubric->

polytics/4015171-ukraina-vihodit-z-konvencii-pro-zaboronu-protipihotnih-min-rada-uhvalila-zakon.html

18. Lippert, W. (2024) Stabilizing Europe's Security Architecture After the Russo-Ukrainian War?. Global Governance Institute Briefing. No. 7. Available at: https://cdn.prod.website-files.com/630b0421cd31598bbf8f31e7/673ddf534c86c26bea1c5618_Lippert-B0724-CAC%20in%20Europe.pdf

19. Belhaj, F. (2025). The New Trump Administration: Selective Multilateralism and the New South's Challenge for Global Relevance. Available at: <https://www.policycenter.ma/publications/new-trump-administration-selective-multilateralism-and-new-souths-challenge-global>

20. Задоя, А. О., Федулова, С. О., Ключник, Р. М. (2024), Архітектура європейської безпеки: нові виклики та загрози: навчальний посібник [Електронний ресурс]. Дніпро: Університет імені Альфреда Нобеля. 297 с. Available at: <https://ir.duan.edu.ua/handle/123456789/3959>

21. UN Security Council Working Methods. The Veto. Available at: https://www.securitycouncilreport.org/un-security-council-working-methods/the-veto.php?utm_source=chatgpt.com

22. Murray, R. (2024). The Case for a Global Defence Bank. Financial Times. December 11. Available at: <https://www.ft.com/content/064b0685-9003-446d-806a-15015978dfed>

23. Now is the moment for a multilateral defence bank. Financial Times. April 9, 2025. Available at: <https://www.ft.com/content/afd25903-e96f-4270-a292-fd2a3671a524>

24. Murray, R. (2024). How a new global defense bank – the ‘Defense, Security, and Resilience Bank’ – can solve US and allied funding problems. Atlantic Council. December 13. Available at: <https://www.atlanticcouncil.org/in-depth-research-reports/report/how-a-new-global-defense-bank-can-solve-us-and-allied-funding-problems/#examination>

25. Roscini, M. (2023). Cyber Operations and the Use of Force in International Law. Oxford University Press. Available at: <https://global.oup.com/academic/product/cyber-operations-and-the-use-of-force-in-international-law-9780199655014?cc=ua&lang=en&#>

26. United Nations Institute for Disarmament Research. (2025). 2024 Outer Space Security Conference Report. Geneva: UNIDIR. Available at: <https://unidir.org/publication/2024-outer-space-security-conference-report/>

27. Centre for Strategic and International Studies. Confidence-Building Measures. Available at: <https://www.csis.org/programs/international-security-program/isp-archives/asia-division/confidence-building-measures>

28. Whitfield, T. (2025) Minilateral Mechanisms for Peacemaking in a Multipolar World: Friends, Contact Groups, Troikas, Quads, and Quints. International Peace Institute. 56 p. Available at: https://www.ipinst.org/wp-content/uploads/2025/05/2505_Minilateral-Mechanisms-for-Peacemaking.pdf

Chapter 2

Global security in a world of change under the influence of development factors and emerging threats

(T. Sergiienko)

Current realities indicate that the dynamics and multifaceted nature of processes unfolding in the modern world create a multidimensional and unpredictable reality of global security, which requires an adequate and effective response not only from governmental authorities but also from the international community. Traditional security mechanisms, which for decades have proven effective under conditions of stability, globalization, and interstate cooperation, are today highly limited and cannot provide a comprehensive response to contemporary challenges.

Conflicts at the global level and geopolitical transformations affect the security of individual regions, increasing the risks of crisis phenomena spreading, destabilization of the socio-political situation, and escalation of local conflicts to the international level. At the same time, the role of international organizations in ensuring global security becomes extremely important, as they perform functions of coordination, monitoring, and crisis response; however, the effectiveness of their actions largely depends on the political will and cooperation of states.

New transnational threats, including terrorism, cyberattacks, and information and hybrid wars, are significantly reshaping traditional notions of security, creating new challenges for national governments and international structures. In addition, demographic, migration, and socio-economic crises exacerbate the vulnerability of states and regions, deepening social inequality, market instability, and tensions in international relations. Thus, contemporary development trends demonstrate that only a



comprehensive, multi-level, and effective approach to ensuring global security, which takes into account political, economic, social, technological, and environmental factors, can address the challenges of the twenty-first century and contribute to the stabilization of the international community.

The study of these very issues constitutes the aim of this chapter

2.1. The impact of global conflicts and geopolitical changes on regional security

Contemporary destructive processes occurring both within states and beyond their borders have a profound political foundation. The main sources of global conflicts are contradictions in political, economic, social, and value-normative spheres. The term «conflict» originates from the Latin word *conflictus*, which literally means «collision» and, in a broader sense, refers to «opposition» or «struggle» [14, p. 46]. In the scholarly literature, a conflict is understood as the lack of agreement between two or more parties regarding a certain object, which becomes the focus of confrontation. Such a state is accompanied by active actions and disrupts normal interaction among the participants. Conflicts can manifest in both latent and overt forms, have a constructive or destructive character, and be either local or escalate to a global scale. A common feature of all these manifestations is the presence of contradictions that pose a threat to the security of participants and the stability of regions. To understand global conflicts, it is appropriate to examine the phenomenon of conflict through an interdisciplinary lens, as this phenomenon attracts the attention of philosophers, psychologists, sociologists, political scientists, and other researchers.

Thus, the concept of ‘conflict’ is studied across various scientific disciplines, which has led to the existence of numerous approaches to its definition. From an etymological perspective, based on the academic explanatory dictionary of the Ukrainian language, a conflict is understood as a «collision», meaning ‘opposition’ or ‘struggle’ [2]. This approach emphasizes the fundamental meaning of the term and highlights the confrontation of opposites.

The conflictological approach defines conflict as a ‘collision, serious disagreements during which participants experience unpleasant feelings or

emotions' [6]. This approach focuses primarily on the emotional component of conflict and the experiences of the participants. The philosophical approach considers conflict as a stage in the development of the category of 'contradiction', when opposites transform into extreme polarities or antagonism [1], emphasizing mutual exclusivity and the philosophical nature of contradictions.

The psychological approach defines conflict as a 'clash of opposing interests (goals, positions, opinions, views) based on rivalry, a lack of mutual understanding, and associated with intense emotional experiences' [19]. This approach highlights rivalry, emotional experiences, and the conditions under which a conflict arises. The political science approach interprets conflict as an 'extreme intensification of contradictions between parties, associated with differences in their social positions and contradictions of interests, goals, and values' [13], emphasizing social positions and systemic opposition.

The sociological approach defines conflict as a 'clash of opposing interests, goals, views, and ideologies between individuals, groups, or classes' and as 'a process of development and resolution of contradictions in people's goals, relationships, and actions' [18]. This approach emphasizes social relationships, both objective and subjective factors, and the collective dimension of conflict.

Thus, the analysis of various scientific approaches to defining conflict allows us to conclude that it is a multifaceted phenomenon, manifesting in political, social, economic, psychological, and other spheres. Despite differences in formulations, the key point is that conflict is always associated with the existence of opposing interests and values, which generate confrontation between subjects.

Global conflicts largely shape the security of regions, as they arise from the intersection of strategic interests of states and other actors in international relations (see Fig. 2.1). The objects of these contradictions may include territories, borders, economic resources, regional dominance, as well as political or ideological values.

Thus, global conflicts and geopolitical changes serve as key factors in shaping the contemporary regional security system. They determine the nature of international relations, influence the distribution of resources and power, and create both challenges and opportunities for the development of new mechanisms for regional and global stability.

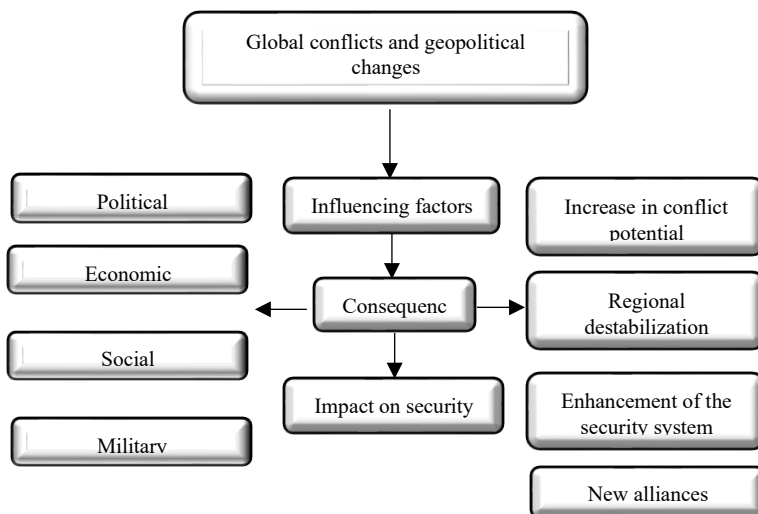


Fig. 2.1. The Impact of global conflicts and geopolitical changes on regional security

Source: compiled by the author

In this context, additional factors that can increase the conflict potential of specific regions become particularly significant: socio-structural transformations, demographic fluctuations, mass migrations, and social inequality. An important factor is also the level of involvement of armed forces, as well as state and non-state actors, since the depth and duration of confrontation directly affect the stability and security of regional communities. These aspects are presented in more detail in Table 2.1.

The analysis of the table allows us to conclude that global conflicts and the associated geopolitical changes create complex threats to regional security. The main factors include contradictions over territories, resources, and values, socio-structural transformations, demographic fluctuations, and the level of involvement of state and non-state actors. The impact of these factors manifests in an increase in conflict potential, threats to stability, and rising risks to the security of regional communities.

Wars and armed conflicts represent only one form of these contradictions, which arise at both the global and international levels. Most contemporary conflicts take the form of armed confrontations, local wars, or military clashes, accompanied by violations of the rights and freedoms of the

population and serious economic consequences. At the same time, not all conflicts escalate to a military phase: many remain political, economic, or socio-political in nature, yet even in these forms, they are capable of creating prolonged instability and increasing the risks of regional destabilization.

Table 2.1

Key Influencing Factors of Global Conflicts and Geopolitical Changes on Regional Security*

Factor	Mechanism of influence	Consequences for regional security
Global conflicts	Intersection of strategic interests of states and international actors	Deterioration of stability, increased risk of violence
Territories and borders	Contradictions over territorial control	Escalation of political and military tension
Economic resources	Competition for access to resources	Economic instability, regional tension
Political and ideological values	Divergences in value systems	Radicalization, spread of conflict potential
Socio-structural changes	Demographic fluctuations, mass migrations, inequality	Increased conflict potential, threat to internal security
Involvement of actors	State and non-state forces, armed formations	Depth and duration of confrontation, impact on regional stability

**Source: compiled by the author*

Analyzing contemporary trends, it should be noted that globalization has a dual effect: on the one hand, it strengthens the interdependence of states, while on the other, it contributes to the intensification of crises, economic problems, and political instability. Geopolitical changes, including the redistribution of centers of power, the formation of new alliances and coalitions, directly affect regional security, increasing the likelihood of local conflicts and escalation of tensions. A particularly illustrative example of the impact of global armed actions on regional security is the Russian-Ukrainian war, which began in 2014 and escalated significantly in 2022. This war has substantially altered the balance of power in Eastern Europe and caused major global consequences: the strengthening of military alliances, the revision of national defense strategies, the growth of defense budgets, and changes in international economic and energy flows. This demonstrates that wars, including regional armed conflicts, can have a global resonance, stimulate the formation of new security systems, and shift the balance of power in the international system.

It should also be noted that contemporary global conflicts redistribute economic flows, alter the balance of power in the world, and impact the international security system, causing the fragmentation of international institutions while simultaneously stimulating the formation of new alliances and coalitions. For Ukraine, which is at the epicenter of the war, this entails the necessity to adapt to new global realities and actively participate in international security alliances and coalitions. International organizations play a crucial role in stabilizing the situation by monitoring crises, coordinating state actions, organizing peacekeeping operations, and contributing to the development of regional security systems. The effectiveness of their actions is often limited by the political will of states and the specifics of military operations; however, active cooperation between international organizations, states, and non-state actors is a necessary condition for reducing the risks of regional destabilization and ensuring stability.

2.2. The role of international organizations in ensuring global security

International organizations play a key role in the contemporary global security system, as they have become an integral actor in international relations and an important instrument of cooperation among states. Their significance lies in creating conditions for the peaceful settlement of disputes, coordinating government actions, developing international legal norms, and organizing collective security measures. As R. Potter notes, the term «international organization» was first used (or began to take shape in academic discourse) by James Lorimer around 1867 [20, p. 804]. Since then, its meaning has undergone significant transformations, leading to the emergence of various scholarly approaches to its interpretation. In contemporary literature, there is no single definition of the concept, as it is examined from legal, historical, and economic perspectives.

According to Yu. Kozak [10], an international organization is an association of states, institutions, or individuals that jointly implement certain programs or objectives, operating according to established rules and procedures beyond national borders. O. Skrypnyk [16] defines an international organization as an institution of multilateral relations, created by at least three participants to achieve common goals, which has permanent bodies and functions in accordance with defined norms, statutes, procedures, and membership rules. L. Tymchenko [17] defines an international

organization as a permanently functioning association of states, established on the basis of a treaty to address specific tasks, possessing its own governing bodies and certain rights and obligations.

A. Voronkova, L. Yerokhin, and L. Ryabenko [5, p. 17] emphasize the voluntary nature of such associations, created in accordance with international law for the purpose of cooperation, possessing an organizational structure and shared objectives. Thus, the various approaches to defining an international organization highlight its multifunctionality, legal foundation, and organizational structure, as well as its role in facilitating international cooperation and achieving common goals.

Thus, the category of «international organization» is multifaceted and examined from various theoretical approaches, reflecting the complexity of its nature and role in contemporary international relations. Despite differing interpretations, there is a common understanding that international organizations serve as important institutional mechanisms for coordinating the actions of states and other actors at the global level. For this reason, it is appropriate to focus on their key objectives and functions, which determine the significance of these structures in ensuring peace, stability, and the development of the international community.

Based on this, the primary goal of international organizations is to ensure peace, stability, and cooperation in the political, economic, humanitarian, and security spheres. They perform informational and advisory functions, fund educational and social programs, promote the development of the rule of law, and facilitate communication between governments and society. The involvement of such structures in conflict resolution enhances trust among states and contributes to the development of preventive diplomacy mechanisms (see Fig. 2.2).

This figure illustrates the comprehensive role of international organizations in ensuring global security, emphasizing that their activities encompass preventive measures, conflict response, and post-conflict recovery. The involvement of various organizations in specific areas of work enables the effective coordination of efforts in human rights protection, disarmament, and the provision of economic and humanitarian assistance, thereby contributing to the promotion of peace and stability in the international environment.

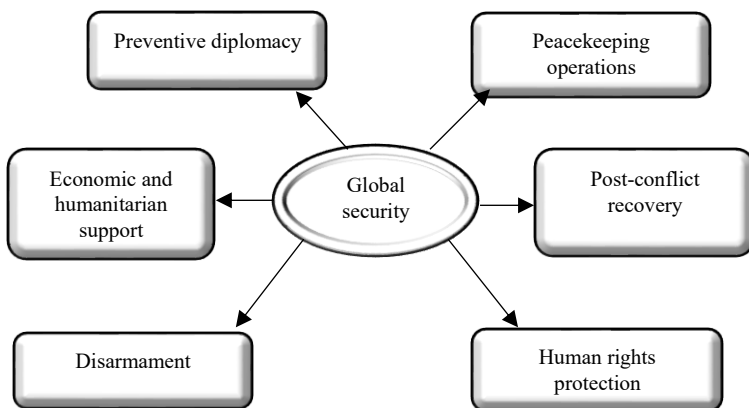


Fig. 2.2. The role of international organizations in ensuring global security

Source: compiled by the author

At the present stage, as O. Kuchyk notes, three main concepts of international organizations can be distinguished: as instruments for achieving common goals and interests, as platforms for conducting events, and as an assembly of participants [11].

In this context, international organizations are often perceived as mechanisms through which states advance their own interests, which largely shapes political processes and reflects the priorities of the most influential members. The need for their establishment arises from the desire to combine the efforts of states in developing joint action programs to address global problems and create conditions for their implementation. At the same time, the execution of these tasks is complicated by the diversity of political, economic, and social systems, levels of development, and national-cultural characteristics of states. Key factors contributing to the emergence of international organizations include the international division of labor, economic integration, political relations between countries, and the globalization of international relations, since global problems affect virtually every country and require collective efforts. Many of these issues intensified in the mid-20th century due to rapid population growth and scientific and technological progress, while in recent times political and military conflicts have become particularly acute.

It should also be noted that contemporary globalization trends demonstrate a decrease in the number of classic international conflicts, while the significance of domestic political conflicts is increasing. These conflicts are associated with separatism, extreme forms of nationalism, religious fundamentalism, transnational terrorism, and international organized crime. Such conflicts arise when individual actors pursue incompatible actions or seek exclusive control over resources or political influence, while still maintaining the possibility of shared perspectives on international relations. As D. Likarchuk notes, many political scientists highlight the growing inability of nation-states to adequately respond to the new challenges of the modern era. Globalization processes undermine state sovereignty, calling into question the traditional system of interstate relations [12].

In such a situation, international organizations come to the forefront, gradually assuming the roles of mediators and coordinators in the field of global security. They are capable of compensating for the limited capacities of national governments and providing a collective response to new challenges.

Recently, the role of international organizations in the field of security has undergone significant changes. They are no longer merely auxiliary instruments for addressing specific issues in state interactions but have become full-fledged actors in international affairs. The importance of their activities in conflict resolution is increasing, with particular attention given to conflict prevention. The mechanisms used by international organizations to resolve conflicts are primarily political, but they are based on international law and contribute to the promotion of peace and stability worldwide.

A special place among international institutions is held by the United Nations (UN), which serves as a global, universal intergovernmental organization with a multifunctional mission. Its main tasks include maintaining peace and security, preventing conflicts, conducting peacekeeping operations, and creating conditions for post-conflict recovery. Other important actors in the field of security governance include the European Union, the Council of Europe, the European Court of Human Rights, the Organization for Security and Co-operation in Europe (OSCE), the World Bank, and the North Atlantic Treaty Organization (NATO). Each of these organizations possesses its own instruments of influence, encompassing military-political, legal, economic, and humanitarian dimensions.

Contemporary globalization trends and the rise of transnational threats have increased the importance of international organizations in preventive diplomacy and disarmament. Their activities are aimed at reducing global conflict, developing democratic oversight of the security sphere, and integrating peacekeeping mechanisms into the broader context of international cooperation.

Thus, international organizations form the institutional foundations of global security by contributing to the reduction of the risks of armed conflicts, ensuring compliance with international law, and creating mechanisms for state interaction in crisis situations. They act not only as arbiters in dispute resolution but also as active actors in international relations, capable of influencing the architecture of the world order. However, the example of the Russian-Ukrainian war has revealed a number of limitations and shortcomings in the role of international organizations. Their inability to counter military aggression, the limited political leverage over aggressors, and their partial dependence on the will of the most influential states have demonstrated the need to reconsider the functions of international organizations.

Contemporary challenges require the development of new approaches to respond to hybrid threats, military aggression, and violations of international law, as well as the enhancement of capabilities for coordinating international efforts, preventive diplomacy, and the prompt provision of economic and humanitarian assistance. These issues are closely linked to a broader range of threats that shape the new architecture of international security and demand effective responses. Transnational challenges include terrorism, cyberattacks, information and hybrid warfare, all of which require coordinated responses by international organizations and states on a global scale.

2.3. Transnational threats: terrorism, cyberattacks, information and hybrid warfare

In the contemporary context of globalization, security issues acquire a new dimension, as states face transnational threats that are not confined by borders and require comprehensive international responses. Terrorism, cyberattacks, information, and hybrid warfare have become key challenges of the 21st century, questioning the effectiveness of traditional security mechanisms.

Transnational threats share several common characteristics. First, they have the potential to undermine the political stability of states as well as their economic and social systems. Second, their nature is such that no single country can effectively counter them without international cooperation.

The main transnational threats have different natures and significantly affect international security. Terrorism, according to O. Voloshchuk [4], involves the use of organized violence or the threat of its use for political, ideological, or religious motives. Such actions can be carried out by officially recognized terrorist groups or by individuals, including so-called 'lone terrorists'. The consequences of terrorism include the destabilization of political regimes and international relations, civilian casualties, the spread of an atmosphere of fear, increased state expenditures on security, and restrictions on civil liberties. Prominent examples include the activities of ISIS and the September 11, 2001 attacks, as well as one of the most high-profile incidents: the downing of Malaysia Airlines Flight MH17 over Donetsk in July 2014. This act, carried out with the involvement of militants from illegal armed groups, resulted in the deaths of 298 people and exemplifies international terrorism that destabilized international relations and exacerbated the security situation in the region.

Cyberattacks are understood as unauthorized intrusions into computer systems, networks, and digital infrastructure with the aim of stealing, destroying, or blocking information, as well as causing harm to critically important facilities. They disrupt the functioning of state institutions, financial systems, energy, and transportation, lead to the theft of confidential data and increased economic losses, and heighten states' dependence on digital security. An example of this is the attacks on Ukrainian government websites in 2022.

In addition to cyber threats, information and hybrid warfare are becoming increasingly significant, combining political, technological, and psychological tools of influence. These strategies are aimed not only at destroying material resources but also at undermining trust, destabilizing society, and weakening state resilience.

Information warfare involves the deliberate dissemination of manipulative materials through traditional media, social networks, and other communication channels to shape public opinion in a favorable way. It causes societal polarization, the spread of fake news and disinformation, undermines trust in state institutions, destabilizes democratic processes, and fosters a distorted sense of identity among the population. An example is Russia's

information campaigns against Ukraine, starting in 2014. Through social networks, anonymous Telegram channels, state-controlled television, and bot networks, false narratives about the ‘illegitimacy of authorities’, ‘foreign control of the country’, ‘the threat of Ukraine’s division’, and ‘betrayal on the front lines’ were spread and continue to circulate.

Hybrid warfare combines traditional military methods with economic pressure, cyberattacks, information manipulation, and support for irregular forces. It blurs the line between war and peace, leads to prolonged destabilization of political systems, economic losses, humanitarian crises, and increases threats to international and regional security.

Particular attention should be given to the phenomenon of hybrid warfare, which combines military and non-military methods of influence. The most striking example is the Russian-Ukrainian war, which scholars define as ‘hybrid’ because it combines traditional and unconventional methods of conducting hostilities: the use of special forces, irregular armed groups, information campaigns, and propaganda. At its initial stage, this war had an ideological character and manifested through political, informational, and economic pressure on Ukraine, aimed at undermining national identity and destabilizing state institutions [9, p. 90].

Subsequently, it escalated into a full-scale armed aggression with extensive use of regular and irregular troops, artillery, aviation, and missile strikes, which has caused and continues to cause significant human losses, infrastructure destruction, and serious deterioration of regional and global security. It is important to note that the tools of hybrid warfare are not entirely new. Similar strategies were employed against the Ukrainian People’s Republic in 1917–1921, demonstrating the cyclical use of such approaches in regional conflicts. Contemporary hybrid warfare is multidimensional, arising at the intersection of interactions between governmental and non-governmental actors, often supported by third countries. Its particular danger lies in the blurring of the frontline, the uncertainty of political and strategic objectives, and the focus on undermining state institutions rather than exclusively conducting combat operations.

Given that these threats exceed the capacities of individual states, international organizations play a key role in countering them. They provide coordination of efforts, establish normative and legal mechanisms, and employ instruments of political and security influence. Leading international organizations are crucial in addressing transnational threats, utilizing diverse areas of activity and response tools.

The United Nations (UN) conducts peacekeeping operations in conflict regions, develops international conventions to combat terrorism and cybercrime, and coordinates global actions against hybrid threats. Key UN instruments include the adoption of Security Council and General Assembly resolutions, the imposition of international sanctions against aggressor states, the provision of humanitarian assistance to affected countries, and the establishment of specialized structures such as the Counter-Terrorism Committee and the United Nations Office on Drugs and Crime.

NATO ensures collective defense and deterrence of aggression, develops strategies to combat terrorism, enhances cyber defense and information sharing among allies, and supports partner countries in strengthening their defense capabilities. The Alliance's main instruments include political-military coordination and joint exercises, the establishment of the Cooperative Cyber Defence Centre of Excellence in Tallinn, the deployment of rapid response forces, and the conduct of counter-terrorism operations.

The European Union (EU) focuses on creating a unified digital space and protecting cyber infrastructure, coordinating actions to combat terrorism, and developing strategies to counter disinformation and information warfare. Key EU instruments include the activities of Europol and the European Cybercrime Centre (EC3), the adoption of cybersecurity directives and regulations such as the NIS Directive and the EU Cybersecurity Strategy, as well as the implementation of sanction mechanisms against terrorist organizations and aggressor states.

The Organization for Security and Co-operation in Europe (OSCE) focuses on arms control and reducing the risks of escalation, preventive diplomacy in conflict regions, promoting election observation and human rights protection, as well as identifying and monitoring hybrid threats. Its main instruments include conducting monitoring missions in conflict zones, organizing dialogue platforms between parties, implementing programs to prevent radicalization and terrorism, and providing expert assistance in the fields of information and cybersecurity [15, p. 102].

International organizations employ comprehensive approaches and instruments to prevent and neutralize transnational threats, thereby supporting global and regional security. Transnational threats represent a multidimensional challenge to the contemporary international security system, as their danger lies not only in the scale and unpredictability of their consequences but also in their global reach. Therefore, the role of

international organizations is decisive, as they establish collective response mechanisms and provide the legal and political framework for combating terrorism, cyberattacks, and information and hybrid wars. The effectiveness of these structures in the future will determine the level of global stability and security.

Thus, transnational threats in the form of terrorism, cyberattacks, information, and hybrid wars shape a new architecture of global insecurity. They undermine not only the security of individual states but also the stability of the international system as a whole. The example of the Russian-Ukrainian war demonstrates that hybrid methods can combine military, informational, and political instruments, creating a prolonged crisis. These processes are closely interconnected with internal factors of instability, including demographic, migration, and socio-economic crises, which directly affect the level of global security.

2.4. The impact of demographic, migration, and socio-economic crises on global security

Wars, economic shocks, and protracted social conflicts increasingly act as catalysts for complex demographic, migration, and socio-economic crises that extend beyond national borders and become a threat to global security. Events of the past decade, in particular the full-scale Russian war against Ukraine, demonstrate that the consequences of such crises overlap, creating long-term risks for international stability.

One of the most notable manifestations of contemporary security challenges is demographic disruption, which emerges under the influence of wars, occupation, and forced migration. A striking example is Russia's armed aggression against Ukraine, which forced millions of people to leave their homes. This has led to population decline, aging societies, loss of labor potential, and distortion of the age and gender structure. States experiencing mass outflows of population face a reduction in economically active citizens, decreased tax revenues, and an aggravation of demographic crises. Recipient countries, in turn, are compelled to adapt their social, educational, and healthcare systems to accommodate these new pressures.

A vivid illustration of this phenomenon is the demographic situation in the temporarily occupied territories of Zaporizhzhia Oblast. While the population in 1991 was approximately 2 million, it had decreased to 1.77 million by 2013 and to about 1.66 million by 2021. After 2022, precise data

are unavailable due to restricted statistics; however, it is estimated that 500–600 thousand people left the region. The remaining population in the occupied territories is around 300–350 thousand, predominantly women, children, and the elderly. Some local residents were forcibly deported to Russia or relocated to other occupied areas.

A significant factor contributing to demographic pressure has been the policy of targeted population replacement. In 2023, Russia initiated the «Zaporizhzhia Virgin Lands» program, launched by Yevhen Balytskyi, which envisaged the relocation of up to 40,000 Russian citizens, including individuals from the Caucasus and Siberia. Changes in the ethnic composition of the population were recorded in Melitopol and Prymorsk. Simultaneously, the number of working-age men decreased due to mobilization, casualties, or evacuation, and the number of school-aged children declined by half. This resulted in a shift in the age balance toward the elderly and women [8].

The migration factor intensifies not only social but also geopolitical tensions. The movement of large population groups from conflict zones alters labor markets, employment structures, and competition for resources. In some cases, this can provoke the radicalization of sentiments or an increase in xenophobia. At the same time, migration has a dual character: it harms donor countries through «brain drain» and loss of human capital, while remittances partially support the economy.

A significant element of the crisis has been internally displaced persons (IDPs). The mass exodus from the temporarily occupied territories of Zaporizhzhia Oblast began in 2022 and involved over 300,000 citizens. Migration waves closely corresponded with escalations in hostilities. By 2024, the pace of displacement had somewhat decreased, yet the process continued. The number of those who have returned to the occupied territories remains uncertain.

For example, the dynamics of internally displaced persons (IDPs) in Zaporizhzhia Oblast reflect the variability of migratory pressure depending on the military situation, while also demonstrating that the region's population showed consolidation, cohesion, and unity in response to an external threat from the very first days of the full-scale war. This was primarily manifested in the operation of humanitarian centers, where the combined efforts of volunteers, regional and city authorities, and local residents ensured the reception and accommodation of IDPs. During the first four months of the war, round-the-clock registration, screening, and assistance were provided for 3,000 to 6,500 displaced persons per day, and

from June onwards, up to 1000 persons per day. From 24 February 2022 to August 2024, a total of 275412 people relocated to Zaporizhzhia, of whom 26.2% (72199) were children [7]. The main regions from which IDPs arrived remained Zaporizhzhia, Kherson, Donetsk, and Luhansk oblasts. According to data as of March 2025, nearly 187000 IDPs were registered in the region, almost half of whom belong to vulnerable population groups [3]. A significant proportion of the displaced population relocated within the oblast: over 51000 from Polohy District, more than 24000 from Vasylivka District, and another 19700 within Zaporizhzhia District itself. The possibility of returning to their homes remains limited due to ongoing hostilities and the occupation of certain territories.

Thus, in 2022–2025, the scale of internal migration varied in accordance with the dynamics of the military situation, access to humanitarian corridors, and prevailing security conditions. The instability of migratory flows and the shortage of personnel in key sectors of the economy and social infrastructure exacerbated regional problems, causing declines in production, rising unemployment and poverty, and increasing the dependence of affected territories on external assistance. During wartime, these processes intensify, complicating the assessment of their impact on the labor market and social services in Ukraine. The full-scale Russian invasion triggered one of the largest socio-economic transformations in the country, altering the demographic structure, labor market pressures, and the functioning of social infrastructure. The consequences of these processes extend beyond the region and directly affect national and global security, highlighting the interconnection of demographic, migratory, and economic crises at the global level (see Table 2.2).

Migration processes caused by war and socio-economic crises have complex economic and social consequences. The reduction of the working-age population due to emigration creates a shortage of skilled personnel in sectors such as IT, education, healthcare, and engineering, slows economic recovery, and limits innovation potential. Labor shortages increase employer costs, affect the competitiveness of the economy, and alter the structure of the labor market. At the same time, remittances from migrants support households and stabilize regions, but they are primarily directed toward consumption, which limits long-term investment.

Mass emigration also exacerbates demographic and social risks. A deficit in social contributions and reduced tax revenues complicates the

funding of social protection systems, healthcare, and educational services, limiting the state's capacity to respond to domestic needs.

Table 2.2

Economic consequences of migration for Ukraine during the war*

Category	Consequences	Short-term effects	Long-term effects
Loss of workforce	Reduction in the working-age population due to emigration	Labour shortages in key sectors such as IT, healthcare, education, and engineering	Slowing of economic recovery due to a deficit of qualified personnel
Growth in demand for jobs	Increased demand for labour in low-skilled sectors such as construction and agriculture	Rising unemployment among highly skilled workers	Occupational downgrading may slow the development of certain industries
Migrant remittances	Inflows of funds from labour migrants supporting households	Reduction of poverty levels among many families	May limit investment in production and innovation due to a focus on consumption
Decline in social contributions	Loss of migrant workers who no longer contribute to social insurance funds	Decreased revenues to pension and social funds	Worsening deficits of social funds and reduced support for the most vulnerable groups
Reduction of social pressure	Migration enables people to avoid the impacts of war and find stability abroad	Lower levels of social tension	Return migration may contribute to social recovery but creates adaptation challenges
Loss of skilled professionals	Emigration of highly qualified workers	Mismatch between labour market needs and available skills	Slowing of scientific, technological, and innovative development
Impact on social infrastructure	Reduced demand for public services for migrants	Limited access to social services for citizens working abroad	Difficulties in accessing healthcare and education for returnees
Post-war migrant integration	Support and reintegration programmes	Preparation for return through vocational and skills training	Creation of incentives for investment and employment of returnees

Source: compiled by the author

Together with labor instability, this creates dependence on external assistance and necessitates the involvement of international financial and humanitarian resources.

Thus, demographic losses, mass population displacement, and socio-economic degradation have a direct impact on global security. The growing number of refugees reshapes international policy priorities, influences defence strategies and humanitarian agendas, while local crises rapidly acquire a transnational character due to the high level of interdependence among states. Effective responses to such threats require coordinated international efforts, the modernization of migration policies, and the development of long-term strategies for demographic and economic recovery. Without a systemic approach, these crises risk creating new centres of instability, undermining the international order and global security.

References

1. Авер'янова, Н. М., Воропаєва, Т. С. (2021). Становлення і розвиток конфліктологічних ідей в історії філософської думки. Молодий вчений. 6(2). С. 128–135. Available at: [http://nbuv.gov.ua/UJRN/molv_2021_6\(2\)_12](http://nbuv.gov.ua/UJRN/molv_2021_6(2)_12)
2. Академічний тлумачний словник української мови. Available at: <http://sum.in.ua/>
3. В Запорізькій області зареєстровано майже 187 тисяч переселенців. Available at: <https://lokatormedia.online/v-zaporizkij-oblasti-zareiestrovano-majzhe-187-tysiach-pereselentsiv/>
4. Волощук, О. Т. (2025). Міжнародні та транснаціональні злочини: концептуально-правові парадигми та виклики протидії й превенції (на прикладі злочину агресії та тероризму). *Науковий вісник Ужгородського Національного Університету*. С. 387–394. Available at: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/53-3.pdf>
5. Воронкова, А. Е., Єрохіна, Л. В., Рябенко, Л. І. (2006). Міжнародні економічні організації: навчальний посібник. К.: ВД «Професіонал». 352с.
6. Дуткевич, Т. В. (2005). Конфліктологія з основами психології управління [навч. посібник]. К: Центр навчальної літератури. 456 с.
7. Запоріжжя займає четверте місце в Україні за кількістю ВПО – міськрада. Available at: <https://suspilne.media/zaporizhzhia/806849-zaporizha-zajmae-cetverte-misce-v-ukraini-za-kilkistu-vpo-miskrada/>

8. Заселення окупантів на ТОТ. Available at: <https://brd.gov.ua/news/132217-zaselennia-okupantiv-na-tot>.

9. Кириченко Ю. В., Сергієнко Т. І., Сластін В. О. (2025). Інформаційні війни як інструмент гібридної агресії: український досвід. *Вісник національного технічного університету України «Київський політехнічний інститут»*. політологія. Соціологія. Право. 1. С. 89–95. Available at: <https://visnyk-psp.kpi.ua/article/view/332563/321559>.

10. Козак Ю. Г. (2007). Міжнародні організації. К.: Центр навчальної літератури. 440 с.

11. Кучик О. (2012). Еволюція поняття міжнародної організації: теоретико-методологічний аспект. Available at: https://intrel.lnu.edu.ua/wp-content/uploads/2015/10/VLNU_Mv_2012_30_6.pdf

12. Лікарчук Д. С. (2020). Роль міжнародних організацій у врегулюванні зовнішньополітичних конфліктів. Available at: <http://international-relations.knukim.edu.ua/article/view/203663/203385>.

13. Політологічний енциклопедичний словник [Текст] (2004) / упор. В. П. Горбатенко; за ред. Ю. С. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка. 2-вид., доп. і перероб. К.: Генеза. 736 с.

14. Ромадікіна, В. С. (2013) Професійна конфліктологія працівників ОВС [Текст]: навч. посіб. / В. С. Ромадікіна, В. О. Лефтеров; за ред. В. М. Бесчастного; Донецький юрид. ін-т МВС України. Донецьк: ДЮІ МВС України. 295 с.

15. Сергієнко, Т. І., Бабарікіна, Н. А. (2021). Міжнародні організації та їх роль у вирішенні глобальних проблем щодо врегулювання політичних конфліктів. *Humanities studies: збірник наукових праць* / гол. ред. В. Г. Воронкова. Запоріжжя: Видавничий дім «Гельветика». Випуск 9 (86). С. 101–108. Available at: <http://humstudies.com.ua/article/view/252005/249400>.

16. Скрипник, О. М. Історія міжнародних організацій: [навч. посібник]. Умань, 2011. 226с.

17. Тимченко, Л. Д. (2012). Міжнародне право [Текст]: підручник. К.: Знання. 631 с.

18. Шевель, І. П. (2021). Конфлікт проти конфлікту: соціологічний аналіз світової проблематики. *Міжнародні відносини: теоретико-практичні аспекти*. 8, С. 238–248. <https://doi.org/10.31866/2616-745x.8.2021.249056>.

19. Що таке психологічний конфлікт і як з ним справитися?
Available at: <https://mentalzon.com/uk/post>.

20. Potter, P. B. (1945). Origin of the Term International Organization.
American Journal of International Law. 39 (4). P. 803–806.

Chapter 3
Geopolitical recession and the path
to a new global security system
(S. Fedulova)

The contemporary international order is experiencing a profound strategic rupture, a phenomenon that Ian Bremmer has described as a ‘geopolitical recession’. This concept encapsulates a condition in which the erstwhile architecture of global governance, historically led by the United States, is progressively losing its efficacy. A geopolitical recession is marked by the erosion of traditional norms, rules, and institutions, which no longer accurately reflect the prevailing distribution of power in the international system. This is manifested in the observable dysfunction of key multilateral institutions tasked with maintaining peace and stability. Furthermore, this period is characterized by the consolidation of regional blocs and the emergence of a more multipolar world, generating heightened instability in both economic and security domains.

Geopolitical recession is closely intertwined with the Fourth Industrial Revolution, in which digital technologies function not only as a driver of economic transformation but also as a catalyst for a fundamental rethinking of the paradigms of conflict and national resilience. Recognizing and conducting an in-depth analysis of the impact of emerging technologies on contemporary conflicts constitutes a critical task for the formulation of effective policies in the fields of peace and security. Ukraine is identified as one of the ‘Digital Leader’ economies and demonstrates a systematic, large-scale approach to digital transformation, which carries significant geopolitical implications.

The war in Ukraine has emerged as a powerful catalyst accelerating the development and practical deployment of low-cost drones and robotic systems designed for attritional warfare. The Ukrainian experience illustrates a global shift toward unmanned technologies that increasingly replace or augment human involvement in the most high-risk operations. These dynamic underscores the critical importance of rapid innovation adoption. The advancement of research and development, enhanced by artificial intelligence, has the potential to significantly compress the technological cycle by reducing development timelines while simultaneously lowering costs. In contemporary conflicts, the pace of technological development and deployment has become a decisive determinant of strategic advantage.

This chapter is devoted to diagnosing the global crisis and providing a critical analysis of the stages involved in the formation of a new international order, ranging from shifts in the economic paradigm to the emergence of a new global security system. It examines the convergence of technologies and the ways in which the boundaries of security are increasingly blurred. The study seeks to demonstrate that overcoming geopolitical recession and establishing a resilient system of global security requires not merely the revision of military doctrines, but a fundamental rethinking of governance under conditions of digital reality. This entails a transformation of regulatory approaches to development that accounts for digital modes of value creation in the market, as well as a departure from entrenched patterns of thinking.

3.1. Diagnosing the global crisis: the era of geopolitical recession

The contemporary international order is undergoing a period of fundamental strategic transformation that can be characterized as a ‘geopolitical recession’. This term was introduced by Ian Bremmer, and in

the report *Top Risks 2017: The Geopolitical Recession* (2017), Bremmer and Cliff Kupchan employed it to describe a condition in which international institutions are weakening, while global leadership and the established order are undergoing significant change [1].

According to Bremmer, a geopolitical recession denotes a prolonged phase characterized by a mismatch between the global balance of power and the institutional structures through which international politics and the global economy have long operated.

The term conceptualizes the current condition as an era defined by the disintegration of the former global order, which was predominantly led by the United States. The essence of geopolitical recession lies in the fact that existing rules of the game and international institutions no longer correspond to the actual distribution of global power. In his address at the 2022 World Economic Forum in Davos, Ian Bremmer noted that post–World War II institutions no longer align with the new global distribution of power, emphasizing that the world has entered a state of ‘geopolitical recession’ [2].

Economic downturns occur with relative frequency – on average every seven to ten years in advanced economies – and are accompanied by well-established response mechanisms, including monetary and fiscal policy instruments. Geopolitical recession, by contrast, constitutes a crisis of systemic governance and legitimacy. It generates profound uncertainty and heightened volatility across the international arena. Bremmer emphasizes that geopolitical cycles are longer and less immediately discernible than economic ones, and that the world is currently experiencing such a phase [3].

An analysis of historical precedents indicates that such periods of systemic volatility inevitably led to radical transformation. For instance, the interwar period (1919–1939) was marked by the collapse of empires and the functional failure of the League of Nations, developments that ultimately culminated in the Second World War. Yet this very breakdown created the conditions for the emergence of new and more resilient alliances and institutions, including the United Nations and the Bretton Woods institutions [3]. This historical experience underscores that the current crisis, while fraught with risks, may also serve as a catalyst for the development of a new and more adaptive global architecture.

Geopolitical recession represents the erosion of the Liberal International Order, which was constructed after the Second World War around three core principles: *the promotion of democratic values, adherence to norms and rules upheld by multilateral institutions, and economic openness* [4]. This erosion

results in the absence of effective global arbitration, intensifying the disregard for liberal norms and accelerating the shift toward a more hard-edged form of Realpolitik 2.0.

Some contemporary scholars distinguish two stages in the evolution of the global order: *the Liberal International Order*, which lasted from 1945 to 1980, and the *Neoliberal International Order*, which came to an end around 2015 [4]. It is widely argued that the implementation of neoliberal approaches became one of the key drivers of the current phase of global instability.

The erosion of this order has been further exacerbated by the resurgence of great power competition – between the United States and the West on the one hand, and China and Russia on the other. Russia, in particular, has sought to undermine the existing international order, which it perceives as predominantly serving Western interests. Attributing the decline of its global influence to advanced Western countries, Russia has, despite its diminishing power, attempted to disrupt the international system through military interventions and cyber operations, including interference in electoral processes within Western democracies.

The most common understanding of the concept of the ‘international order’ is based on its definition as a system of clearly established *principles, norms, and institutions* that shape the fundamental relations among states [5]. *Dominant states* or coalitions of states exert decisive influence over the formulation of *rules and principles* that determine the character of interactions between countries within the international order [6, 7].

These rules and principles are grounded in the *societal norms* of the most powerful states, whose values and beliefs provide reference points for *international behavior* [4, 7]. The norms themselves emerge from the demands and needs of individuals and social groups within society, which, through political institutions, shape the ‘*state priorities*’ – the primary *social and strategic objectives of the state* [8].

Order is also defined by the *set of ideologies* that permeate political decisions, strategies, and the activities of supporting groups [8; 9]. Consequently, the international order depends not only on the material capabilities of states but also on prevailing norms and *ideological foundations* that shape the system of *political, economic, and social interaction* – that is, contemporary globalization.

The opportunities for participation in transnational economic, social, and cultural processes generated by globalization have become a key source

for determining the objectives and priorities of both domestic groups and state governments [10].

The norms and principles established by leading powers influence other countries, gradually permeating domestic social processes and shaping state behavior in the international arena. As a result, global interactions among state and non-state actors contribute to the consolidation of existing rules, principles, and norms of the international order.

It is evident that geopolitical recession manifests itself through the dysfunction of key multilateral institutions tasked with maintaining peace and stability. The most salient trends include the following:

- paralysis of the UN Security Council;
- NATO's adaptation to emerging threats;
- geopolitical shifts within the European Union.

The UN Security Council serves as a key international institution established to maintain global peace and security. However, it is increasingly criticized today for its ineffectiveness in addressing contemporary challenges. In particular, the frequent use of the veto has led to a de facto paralysis of its operations, as clearly demonstrated by the Council's inability to respond promptly to conflicts in Ukraine and the Gaza Strip. This inaction indicates that established international norms no longer carry binding authority for the world's leading powers.

The weakening of the UN Security Council's role, coupled with the emergence of new competing military alliances beyond the influence of the G7, reflects the erosion of the existing global security architecture.

The most powerful military alliances, such as NATO, are compelled to fundamentally recalibrate their strategic orientation. Although conventional military aggression against the Alliance is considered unlikely, NATO continues to undergo reform and modernization in order to address an expanding spectrum of non-conventional challenges [11].

Contemporary global threats differ significantly from those envisaged at the time of the signing of the North Atlantic Treaty in 1949. These now include the proliferation of weapons of mass destruction – chemical, biological, radiological, and nuclear – as well as terrorism and emerging hybrid threats such as cyber risks, energy insecurity, and maritime piracy. NATO's 2010 Strategic Concept emphasizes that crises and conflicts beyond the Alliance's territory can directly affect its security by fostering extremism and transnational criminal activity [11].

The European Union is likewise undergoing a recalibration of priorities in its external policy. According to existing analyses, the EU's Common Security and Defence Policy increasingly relegates democracy-related commitments in favor of more hard-edged security priorities [12]. This shift reflects a broader drift of the EU toward a more explicitly geopolitical posture, driven by external factors such as intensifying competition, the presence of disruptive actors, and the disregard for international norms by certain states [12]. The turn toward Realpolitik 2.0 at the very core of the liberal bloc constitutes further evidence that multilateral institutions are responding to geopolitical recession by shifting their focus from universal values toward the protection of their own interests.

It should also be noted that the period of geopolitical recession is characterized by the consolidation of regional blocs and the rise of multipolarity, developments that generate instability at both economic and security levels.

Consolidation of an anti-Western bloc. The emerging multipolar world lacks a unified architecture; instead, it facilitates the formation of parallel defense and economic frameworks. The war in Ukraine and the Western response to it have intensified the trend toward the consolidation of an anti-Western bloc. Russia, for example, has actively sought to reposition itself by strengthening ties with China, India, and North Korea (notably through platforms such as the Shanghai Cooperation Organisation – SCO), thereby reaffirming its integration into a growing bloc that challenges the existing world order [13]. Any territorial concessions by Ukraine resulting from external pressure would establish a dangerous geopolitical precedent by signaling that borders can be altered through force, with far-reaching and long-term global consequences.

Since the end of the Second World War, the United States has consistently upheld the principles of sovereignty and territorial integrity as the foundation of the international order, opposing any attempts to alter borders through the use of force. Any settlement that effectively rewards the aggressor would constitute a departure from this fundamental principle. The war in Ukraine is therefore of critical importance for the preservation of the rules upon which the global system is based. If it becomes acceptable for states to change borders by military means, the world would become significantly less stable, marked by persistent threats to smaller states and the predominance of force over diplomacy.

Allowing Russia to retain control over occupied territories would leave Ukraine vulnerable to renewed aggression and further fuel the Kremlin's expansionist ambitions. It could also provoke a rift between the United States and Europe – an outcome that Russia actively seeks [13]. Such a scenario would undermine the international order, as authoritarian states may conclude that border revisionism and violations of international law no longer entail meaningful consequences.

If the United States were to prioritize political expediency over principles, it would risk witnessing the collapse of the very system it has helped build over decades.

Economic fragmentation. In the economic dimension, geopolitical recession manifests itself through rising instability and the transformation of economic instruments into tools of political leverage. The intensification of geopolitical rivalry and uncertainty in fiscal and trade policy – particularly on the part of the United States – have contributed to increased volatility in global financial markets.

Analysts highlight two key risks: the potential escalation of a trade war resulting from higher tariffs, and the intensification of tensions surrounding Taiwan [14]. At the same time, the United States has increasingly favored regulatory arrangements over comprehensive trade agreements, while China has actively expanded its influence in Southeast Asia, Africa, and Latin America through bilateral and regional initiatives. This trend reflects a broader process of deepening economic regionalization.

As a result, an institutional vacuum is emerging, which encourages the formation of new regional blocs. Due to declining trust in global institutions, states increasingly resort to creating alternative mechanisms of cooperation – regional alliances or bilateral agreements – as means of self-protection. If this dynamic persists, global interaction and security will be grounded not in universal norms, but in shared political and value-based orientations. Consequently, the international security system will become fragmented, structured around situational alliances and converging interests rather than the principles of international law.

A comparison of the key parameters of the Liberal International Order and the period of geopolitical recession can be presented as follows (Table 3.1).

Table 3.1

Comparative Overview of International Orders*

Parameter	Liberal International Order	Geopolitical Recession Period
Hegemony and Leadership Structure	Unipolarity (the United States), clear institutional leadership	Multipolarity, lack of clear leadership, regional power centers
Economic Principles	Economic openness, globalization (WTO, IMF)	Fragmentation, increased protectionism, economic weapons (sanctions)
Institutional Effectiveness	Norm compliance and effective multilateral institutions	Paralysis of the UN Security Council, use of veto, rise of regional and parallel structures
Key Challenges	Conventional threats, proliferation of weapons of mass destruction	Hybrid conflicts, cyber warfare, autonomous systems, climate change

**Source: compiled by the author based on [1, 3–8]*

3.2. Technological convergence and the blurring of security boundaries

Contemporary technological advances that integrate artificial intelligence (AI) with Big Data, cyber and information operations, nanotechnologies, biotechnology, and robotics are creating a fundamentally *new paradigm of conflict* [15]. In this new context, traditional boundaries between war and peace, between military and civilian spheres, and between physical and digital security are rapidly blurring. This necessitates a comprehensive, systemic approach to security by states and international alliances.

Cyberspace is no longer perceived merely as a virtual domain – it has become a fully operational battlefield with tangible real-world consequences [15]. Accordingly, effective diplomacy and peacebuilding initiatives require a deep understanding of technological factors, including the very structure of the cyber domain itself.

Armed groups and non-state actors are increasingly utilizing new fintech tools and cryptocurrencies to finance their terrorist objectives, taking advantage of relative anonymity and the lack of regulatory oversight.

However, diplomats and peacekeepers often underestimate the threats posed by revolutionary technologies. This is due to an excessive focus on traditional notions of the balance of power, a lack of creative thinking reinforced by a culture of caution among political elites, and a detachment from local communities where violence originates. Insufficient technical literacy, in turn, hampers understanding of the mechanisms through which

emerging technologies are deployed and the ways in which they can exacerbate conflicts [15].

For diplomats and peacekeepers, it is crucial to understand that cyberspace is no longer merely a digital environment – it has become an arena of real-world conflict.

Amid rising geopolitical threats, *digital transformation* (DT) is increasingly viewed not simply as a tool for enhancing efficiency, but as a strategic necessity – a key factor for the survival of both businesses and state institutions. Digital transformation provides long-term competitive advantage by fundamentally rethinking customer experience, operational processes, business models, and governance systems.

Resilience in the Digital Era is based on the synergistic use of breakthrough technologies.

1. *Artificial Intelligence (AI) and Big Data Analytics.* AI plays a leading role in enabling digital transformation (DT). Big Data analytics provides deep insights into market trends and internal operations, allowing organizations to develop strategies based on precise forecasts. AI delivers real-time intelligent analytics, offering predictions, recommendations, and actionable insights without the need to invest in large-scale in-house servers. This enables decision-makers to act swiftly and decisively in response to emerging risks.

2. *Cloud Computing.* Cloud technologies are critical because they provide virtually unlimited information capacity, addressing scalability challenges. They offer the necessary infrastructure for expansion and serve as a platform for integrating computationally intensive technologies such as AI and the Internet of Things.

3. *Internet of Things (IoT).* IoT connects devices and machines that exchange digital data within a unified network. AI-driven business systems continuously process this data to identify patterns, trends, and correlations. Through machine learning, system performance improves progressively over time.

4. *Enterprise Resource Planning (ERP) Systems.* Modern cloud-based ERP solutions function as the “brain” of business digital transformation. They integrate all core company processes – finance, HR, manufacturing, and supply chain – into a single system. When combined with AI technologies, ERP systems can not only manage Big Data but also analyze and learn from it, providing deep real-time insights to support informed decision-making.

Assessment of the situation indicates that successful digital transformation (DT) is a direct prerequisite not only for economic competitiveness but also for the operational resilience of states and businesses in conditions of hybrid warfare. Cloud-based intelligent analytics and integrated ERP systems provide real-time data governance, which is essential for rapid managerial response. Accordingly, the speed of transformation becomes a critical strategic advantage over outdated, slow systems, and the transformation itself reshapes the very economic paradigm (Fig. 3.1).

Evaluating and understanding the impact of emerging technologies on the nature of violence is a key precondition for developing effective strategies to strengthen peace and security. In the contemporary world, the boundaries between war and peace, between military and civilian spheres, and between physical and digital security are gradually eroding (Table 3.2).

Table 3.2

The Impact of Key Digital Technologies on Global Security*

Technology	Critical Role in Business Digital Transformation	Strategic Role in Global Security
Artificial Intelligence (AI)	Personalization, intelligent analytics, process automation	A new conflict paradigm, autonomous weapons systems, and advanced analytics for military and security purposes
Cloud Computing	Scalability, cost reduction, infrastructure for Big Data	Critical infrastructure for governments and military systems, cyber resilience, and data security
Big Data	Market trend forecasting, risk management, customer-centricity	Behavioral analysis, intelligence gathering, forecasting of social and economic risks
Internet of Things (IoT)	Real-time data collection, optimization of production and logistics	Integration of military devices, supply chain integrity, management of critical infrastructure

**Source: compiled by the author based on [11, 13, 15-17]*

Overcoming the consequences of the geopolitical recession and establishing a sustainable long-term global security system require a comprehensive overhaul – from reforming governance structures and regulatory approaches to investing in human capital.

It should also be noted that digital transformation represents a fundamental cultural shift, compelling organizations to continuously

challenge the status quo, embrace experimentation, and become accustomed to potential failures.

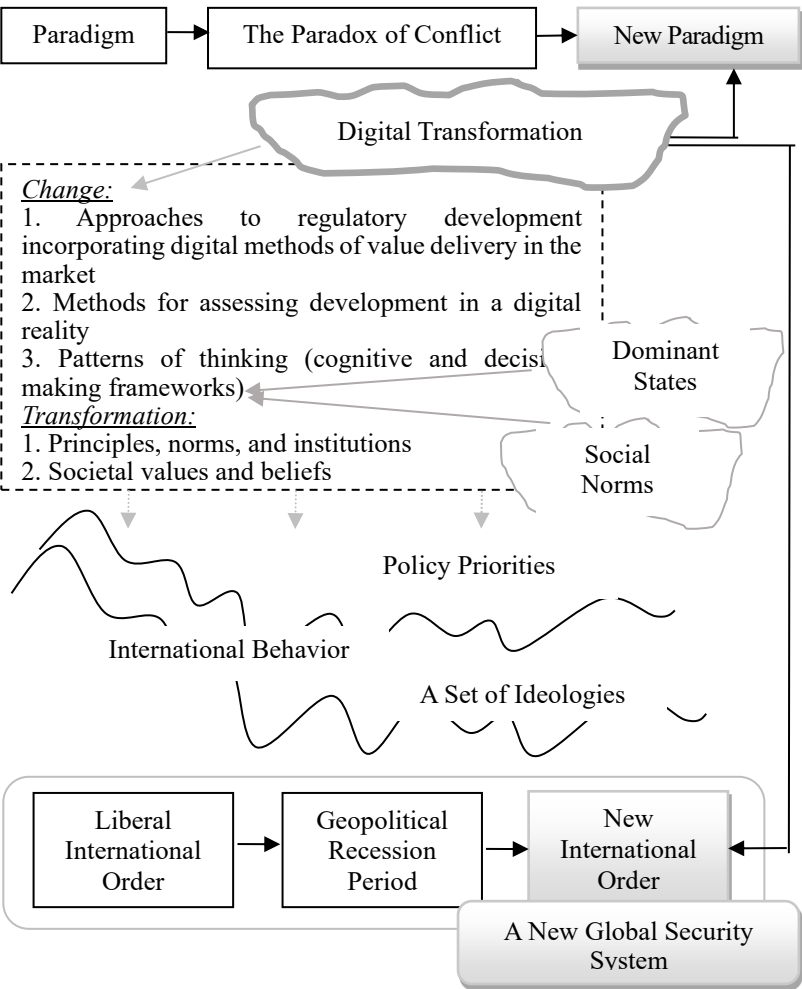


Fig. 3.1. Stages in the formation of a new international order: from economic paradigm shift to a new global security system

Source: compiled by the author

This represents a cultural adaptation and resilience that impacts all areas and functions of business. Corporate culture must be oriented toward flexibility, project-based work methods, proficiency in digital tools, and the cultivation of creative thinking.

Traditional linear implementation methodologies, which rely on clearly defined sequential stages, conflict with the need for rapid responsiveness in the digital era. In contrast, digital transformation in the security sector and public administration requires Agile approaches. Agile methodologies focus on the rapid deployment of technologies (even if imperfect), continuous feedback, and iterative improvement, which are critical for ensuring repeatability and scalability of processes.

3.3. Towards a new global security system: policy and strategic recommendations

Research indicates that the contemporary international system is experiencing a phase of geopolitical recession – profound structural crisis caused by a mismatch between the actual distribution of global power and an outdated governance architecture. This dissonance has led to the functional paralysis of key institutions (notably the UN Security Council), accelerated regionalization and the formation of value-oriented alliances, and intensified the use of economic instruments as tools of geopolitical leverage.

Existential-scale threats are amplified by the convergence of breakthrough technologies, such as artificial intelligence, Big Data, and the Internet of Things, with military and hybrid conflicts. In this new reality, digital transformation is no longer merely a tool for efficiency improvement but has become a strategic condition for the survival of states and organizations. The critical challenge lies in bridging the gap between the exponential pace of technological change and the slow, linear nature of international regulation.

Research on national security strategies demonstrates that states interpret the concept of security differently and consequently have varying priorities regarding the application of advanced technologies in this domain. Some countries exhibit caution in adopting innovative technologies, while others actively acknowledge the need to integrate a wide range of modern technologies into military operations or, at a minimum, adjust their technological priorities accordingly [16].

It should be noted that the West and NATO countries do not constitute a unified technological bloc with identical preferences. Technological priorities appear to be influenced by threat perceptions, the geopolitical positioning of each state, and historical experience in adopting new technologies.

Future success will depend on societies' ability to undertake institutional, managerial, and cultural adaptation, transforming technological innovations into the foundation of systemic resilience.

The new security architecture must address the structural tension between the exponential pace of technological development and the traditionally slow cycles of international regulation. Business and technology often operate under a 'bias for action', valuing speed over extensive research, as many decisions are reversible [17]. International institutions, by contrast, are based on consensus and the gradual establishment of norms.

For effective management of technological risks, particularly cyber threats and the development of autonomous weapon systems, the international community must act systematically and in a coordinated manner. This entails:

1. Preventing regulatory fragmentation. It is crucial to avoid uncoordinated, duplicative, or conflicting cybersecurity requirements [18], as they create barriers to cooperation and reduce the effectiveness of the global security system.

2. Implementing adaptive standards. Priority should be given to establishing international, voluntary, and consensus-based standards grounded in best industry practices, enabling rapid responses to technological changes.

3. Ensuring balanced AI regulation. Formats such as the G7 should take a leading role in creating universal norms for autonomous weapons and the ethical use of artificial intelligence [15]. This requires the adoption of flexible approaches (Agile methodologies) that allow standards to be regularly updated in response to the pace of innovation.

4. Strengthening international cybersecurity cooperation. It is essential to maintain open cross-border data flows to facilitate real-time threat intelligence sharing [18]. Modern cloud-based AI solutions already play a key role here, enabling proactive detection of cyberattacks and anomalies.

In a multipolar world, building a new architecture of global security is impossible without a genuinely inclusive approach that actively engages Global South countries. Prolonged Western dominance has often produced

patronage-based cooperation models that did not always reflect the real interests of partners [19, 20].

In the context of growing polarization between the United States and China – where Beijing is no longer content with the role of an economic superpower and seeks to shape a new international order through BRICS+, the Belt and Road Initiative, and various informal alliances – Europe must expand its network of partnerships. Peripheral states, such as Indonesia and Brazil, could serve as strategic intermediaries for Europe, enabling the continent to maintain influence in a world undergoing a fundamental rethinking of global relations [21].

The contemporary international order requires a rethinking of interaction principles:

1. *Abandoning patronage.* The West must overcome outdated models inherited from its era of dominance and develop equitable partnerships based on mutual benefit and the needs of all parties [19].

2. *Prioritizing the rule of law.* The European Union, in cooperation with distant partners, should assess the reliability of partnerships primarily through the lens of adherence to the rule of law [22].

3. *Supporting local leadership.* Western initiatives should focus on fostering mutual understanding, knowledge exchange, and the development of local ownership, thereby enhancing the effectiveness of development programs and ensuring stability in the field of international security [19].

Effective management of adaptation at the national level also requires a systemic approach that integrates three key dimensions: assessment of digital maturity, investment in human capital, and a citizen-centered orientation. Regular diagnostics of the digital readiness of public and private institutions ensures coordinated actions within international alliances. The development of digital leadership and managerial competencies establishes a skilled workforce for transformation, while the adoption of citizen-centric principles enhances transparency, efficiency, and social trust, laying the foundation for a resilient, agile, and competitive state.

It is essential to implement a systematic practice of regularly assessing the digital maturity of governmental and private organizations using recognized international methodologies [23]. Particular emphasis should be placed on personnel readiness for digital change and the flexibility of IT infrastructure, as the level of digital maturity is gradually becoming an informal standard for operational interoperability among partners and allies.

The state should promote programs aimed at cultivating a digital culture, leadership, and strategic thinking among managers and civil servants. This approach helps address workforce shortages, reduce resistance to organizational change, and ensure the sustainability of transformation processes, as the human factor is a critical determinant of success.

The implementation of digital transformation principles – such as citizen-centricity, process automation, and service personalization – can enhance transparency, efficiency, and trust in institutions. At the macro level, these measures contribute to strengthening state legitimacy and social resilience during periods of global instability.

References

1. Sile, A.W. (2017). Prepare for a ‘geopolitical recession’ in 2017: Eurasia Group. CNBC. Available at: https://www.cnbc.com/2017/01/04/prepare-for-a-geopolitical-recession-in-2017-eurasia-group.html?utm_source=chatgpt.com
2. Pomeroy, R., Bruce-Lockhart, A. (2022). We are in a geopolitical recession’ - Ian Bremmer on globalization, populism and the power of crisis. World Economic Forum. Available at: https://www.weforum.org/stories/2022/06/ian-bremmer-crisis-geopolitical-recession-davos-2022/?utm_source=chatgpt.com
3. Geopolitical Recession: Navigating Risks, Seizing Opportunities, Moving Forward. Blogs. Times of Israel. 2025. Available at: <https://blogs.timesofisrael.com/are-trumps-tariffs-working/>
4. Ramirez, C. H. (2025). The Post-War Evolution of Globalisation and International Order: From Liberal to Neoliberal International Order. Taylor & Francis Online. Available at: <https://www.tandfonline.com/doi/full/10.1080/13600826.2025.2470838#abstract>
5. Ikenberry, G. J. (2019). After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars. Princeton, NJ: Princeton University Press.
6. Kupchan, C. A. (2014). Unpacking Hegemony: The Social Foundations of Hierarchical Order. Power, Order, and Change in World Politics. In Power, Order and Change in World Politics, edited by G. J. Ikenberry. Cambridge: Cambridge University Press. PP.19–60.

7. Moravcsik, A. (2008). The New Liberalism. In *The Oxford Handbook of International Relations*, edited by Christian Reus-Smit and Duncan Snidal, Oxford, UK: Oxford University Press. 234–254.
<https://doi.org/10.1093/oxfordhb/9780199219322.003.0013>
8. Gerstle, G. (2023). *The Rise and Fall of Neoliberalism: America and the World in the Free Market Era*. New York, NY: Oxford University Press.
9. Rodrik, D. (2011). *The Globalization Paradox. Democracy and the Future of the World Economy*. Norton&Company. 368 p.
10. Rodrik, D. A (2024). *New Trilemma Haunts the World Economy*. Project Syndicate. Available at: <https://www.project-syndicate.org/commentary/new-trilemma-of-climate-change-global-poverty-rich-countries-middle-classes-by-dani-rodrik-2024-09>
11. Official website. NATO. Available at: <https://www.nato.int/cps/en/natohq/news.htm>
12. Kalash S. Yash. (2025). *The G7 Reimagined: Navigating a Multipolar World*. Centre for International Governance Innovation. Available at: <https://www.cigionline.org/articles/the-g7-reimagined-navigating-a-multipolar-world/>
13. Radpey, L. (2025). *A US concession to Russia on Ukraine would usher in a new world order*. London School of Economics and Political Science. Available at: <https://blogs.lse.ac.uk/usappblog/2025/10/13/a-us-concession-to-russia-on-ukraine-would-usher-in-a-new-world-order/>
14. Seydl, J. (2025). *Five factors we use to track recession risk, and what they say now*. JPMorgan Chase & Co. Available at: <https://privatebank.jpmorgan.com/nam/en/insights/markets-and-investing/five-factors-we-use-to-track-recession-risk-and-what-they-say-now>
15. Cheatham, A. (2024). *How Disruptive Technologies Are Changing Peace and Security*. The United States Institute of Peace. Available at: <https://www.usip.org/publications/2024/06/how-disruptive-technologies-are-changing-peace-and-security>
16. Korkusuz, A. K., Schörnig, N., Reinhold, Th., Suckau, L. (2024). *A Global Perspective on New Military Technologies in National Security Strategies*. Monitor. Available at: <https://monitor.enrtrmscontrol.org/en/2024/a-global-perspective-on-new-military-technologies-in-national-security-strategies/>
17. *How to Build a Digital Transformation Roadmap for Your Organization*. Amazon Web Services. 2025. Available at:

https://aws.amazon.com/executive-insights/content/mapping-your-digital-transformation/?nc1=h_ls

18. ITI Shares New Cybersecurity Policy Roadmap for Governments Globally. Information Technology Industry Council v4.0. 2025. Available at: <https://www.itic.org/news-events/news-releases/iti-shares-new-cybersecurity-policy-roadmap-for-governments-globally>

19. The Global South in the World Order. The Henry L. Stimson Center. 2025. Available at: <https://www.stimson.org/project/global-south/>

20. Федулова, С. О., Резяпов, К. І. (2025). Продовольча дипломатія та голодування як воєнний злочин. Наука, технології, інновації: Науковий журнал. №1(33). С. 13–18. <http://doi.org/10.35668/2520-6524-2025-1-02>

21. Rethink Perspectives: how should investors respond to the rise of a new world order? Lombard Odier. 2025. Available at: <https://www.lombardodier.com/insights/2025/july/rethink-perspectives-how-should-investors-respond-to-the-rise-of-a-new-world-order.html>

22. Федулова, С. О., Береза, О. Д. (2023). Правове регулювання міжнародних торговельних відносин: межі використання джерел права. Право і суспільство. №6. С. 344–348. <https://doi.org/10.32842/2078-3736/2023.6.50>

23. Шимановська-Діанич, Л. М., Лозова, О. В. (2024). Вплив цифрової зрілості на трансформацію бізнес-процесів підприємств в умовах змін економіки України. ECONOMICS: time realities. №2(72). С. 74–84.

Chapter 4
Security of cross-border territories under the conditions
of the Euroregional cooperation development
(S. Leonova)

The study focuses on identifying the essence and role of cross-border cooperation and Euroregional interaction in ensuring the development of border areas and in shaping a cross-border security system. It elucidates the content of the concepts of ‘cross-border cooperation’ and ‘Euroregion’, defines the goals, principles, and directions of their activities, and analyzes the factors influencing the effectiveness of interaction between border regions. Particular attention is paid to cross-border security issues as a component of the overall security system, including their political, economic, environmental, humanitarian, and criminogenic aspects. The subject of this chapter’s research is the impact of Euroregional cooperation on the development of border territories and on ensuring their security in the context of European integration.

4.1. Identification of the concept of security in the context of cross-border cooperation

Cross-border cooperation encompasses any joint actions aimed at deepening good-neighbourly relations between communities or authorities operating under the jurisdiction of two or more states. It is carried out within the scope of powers vested in territorial communities or public authorities in accordance with national legislation, primarily through the conclusion of relevant agreements or arrangements. Border regions are territories inhabited by communities connected through multifaceted relations yet separated by state borders. Despite political differences between the countries to which these communities belong, they share similar socio-economic, cultural, political, and legal challenges. Therefore, a key principle of international cross-border cooperation is the establishment of such relationships and

contractual ties in border areas that enable the joint resolution of common tasks [14].

Euroregions represent one of the highest organizationally and legally formalized forms of cross-border interaction between neighbouring self-governing territorial communities and local public authorities in the border regions of European countries. They function as international associations comprising several administrative-territorial units of adjacent states.

The term “Euroregion” derives from the oldest cross-border cooperation initiative, “Euregio,” established in 1958. In line with EU principles, Euroregions are intended to promote the generation of collective benefits beyond state borders [10, p. 48].

The main objective of establishing Euroregions is to intensify cross-border dialogue between neighbouring states, in particular through initiating activities that foster closer ties between local communities and authorities in border areas, expanding economic and humanitarian cooperation, developing infrastructure and communications, promoting cultural and educational initiatives, tourism, and environmental protection. The functioning of Euroregions turns them into distinctive ‘bridges’ of European integration, which, through their activities, accelerate its political advancement.

The formation of Euroregions is based on institutional arrangements between national and local authorities, as well as on informal ties between professional or academic associations aimed at cooperation in border areas. Euroregions are characterized by the following features:

- they serve as a formalized organizational structure of cross-border cooperation between regional or local authorities, with the possibility of involving economic and social partners;
- agreements on the development of cross-border cooperation with neighbouring regions of adjacent countries are implemented within Euroregions;
- the establishment of Euroregions necessarily involves recognition of existing state borders and compliance with the national legislation of participating countries;
- a Euroregion functions as a cross-border structure that unites administrative units of specific territories for the purpose of cooperation;
- the boundaries of a Euroregion are determined by shared problems, the nature of interconnections in various areas of activity, and the willingness of individual institutions and communities to cooperate.

The Association of European Border Regions (AEBR) is an international non-governmental organization established to unite cross-border regions to strengthen their role in pan-European cooperation. Its key tasks include:

- implementation of joint projects and programmes, attraction of funding, and management of resources;
- organization of events related to cross-border interaction;
- participation in addressing cross-border cooperation issues and support for key initiatives;
- development and implementation of joint activities;
- advancement of the “Centre for European Border and Cross-Border Regions” in close cooperation with EU institutions and the Council of Europe;
- informing political actors and the public in Europe about cross-border interaction issues.

Euroregional cooperation is one of the key instruments for shaping new interstate and interregional relations in Europe. The legal basis for these processes consists of multilateral (international) agreements, in which one of the fundamental principles is the promotion and consolidation of diverse forms of cross-border cooperation.

An analysis of academic studies and existing legal and regulatory acts allows for the identification of the following core principles of cross-border cooperation:

- respect for state sovereignty, territorial integrity, and the inviolability of borders;
- clear delineation of functions and responsibilities among participants in cross-border interaction;
- consideration of the powers of the parties and the rights of all participants when concluding agreements;
- coordination of interests at the national, regional, and local levels;
- joint elimination of political, economic, legal, administrative, and other barriers to cooperation;
- responsibility of all levels of government in addressing problematic issues;
- partnership, comprehensiveness, and effectiveness of interaction;
- prioritization of adequate financial, legal, security-related, and informational support.

Establishing effective cooperation between border regions requires significant efforts by local authorities and support from the national governments of all states sharing common borders. By uniting into cross-border regions, such territories encounter a number of factors that determine the effectiveness of their activities; however, not all of these factors can be fully predicted or eliminated at the regional or central government levels. For this reason, the study of cross-border security issues becomes increasingly relevant, particularly the identification of key threats that affect the development of border regions, their interaction, and may have negative consequences for economic, social, cultural, and environmental spheres.

In this context, cross-border cooperation can be viewed in two dimensions: as a mechanism for the development of border territories and as an instrument for enhancing the protection and security of state borders.

For a long time, security policy in both the East and the West focused on arms control and the maintenance of stability, a focus that was especially evident during the Cold War. Awareness of its potential consequences contributed to the initiation of European security and cooperation processes, which laid the foundation for stabilizing the European space.

Today, security is one of the key tasks of states and the international community, stimulating the search for effective ways to ensure it. For small and medium-sized countries lacking sufficient resources for independent defence, joining collective security systems and participating in political and military alliances becomes particularly relevant. Such steps require a certain limitation of sovereignty but are undertaken voluntarily in the interests of the common good.

Collective security is an extremely important component of the European Union's policy, as ensuring peace and stability concerns every country. Its principles include the joint preservation of peace, rejection of the use of military force, peaceful settlement of conflicts, as well as the application of political, diplomatic, and economic sanctions against potential aggressors.

The academic literature contains numerous definitions of the concept of 'security', highlighting its multidimensional nature. Dictionaries most often interpret it as a state of a country or community capable of resisting internal and external threats. The term itself originates from the Latin *securitas*, meaning 'absence of fear, calmness'. In the Oxford Dictionary, 'security' is defined as:

- 1) freedom from or protection against danger or anxiety;

2) measures taken to ensure the safety of a state, an individual, or property.

The social sciences regard security as the ability to survive, preserve identity, maintain independence, and develop. Researchers note that security is a basic human and societal need, associated with freedom from fear and external pressure. In particular, Z. S. Varnalii defines security as the degree of protection against negative influences of internal or external origin, while T. A. Maliarenko emphasizes its significance as freedom from fear and hostile influences [5, 9].

In this context, cross-border security is understood as a state of freedom from negative internal and external influences that are common to several territories separated by a state border. A narrower concept is that of 'security of cross-border cooperation', which refers to protection from adverse impacts on any joint actions aimed at developing good-neighbourly relations and concluding relevant agreements.

The key difference between these terms lies in the fact that cross-border security focuses on identifying threats to border territories as a whole, whereas the security of cross-border cooperation concerns the practical organization of interaction between border communities and public authorities.

The formation of cross-border security is an essential precondition for effective interaction among communities of different countries. It should facilitate the development of economic, social, and cultural contacts, improve the quality of life of populations in border regions, and reduce the negative effects of the existence of state borders. At the same time, this phenomenon is complex and multidimensional, as it encompasses various security domains and spheres of social activity.

By generalizing theoretical approaches, it is possible to determine the place of cross-border security within the overall security system and to identify its components. In analyzing the economic security of Euroregions, four levels can be distinguished: the mega level, the macro level, the meso level, and the micro level. A similar approach is appropriate for the security system as a whole. In particular, cross-border security emerges as a fundamentally new level located between national and regional security.

It can be identified according to two criteria:

- a) the subject level – mega, national, meso, and micro levels;

- b) the structural composition – political, economic, military, scientific and technological, environmental, humanitarian, demographic, and information security.

Thus, cross-border security possesses specific characteristics that differentiate it from regional security and should be considered an independent component of the overall security system.

Ensuring cross-border political security acts as a factor in stabilizing relations between border regions and promotes the establishment of constructive political dialogue between territories of different states. This creates the necessary preconditions for effective socio-economic development of communities residing in border areas.

Cross-border scientific and technological security is associated with the development of scientific activity within cross-border territories. Although each country primarily focuses on its own priorities in science and technology, when enterprises operating in these territories are integrated into unified technological processes, compliance with international standards in the field of intellectual property and patent protection becomes crucial. This necessitates the search for compromises between the parties to ensure effective cooperation and joint scientific progress.

Environmental security in cross-border territories is an objective prerequisite for sustainable development, as natural disasters and environmental catastrophes do not recognize state borders and inevitably affect neighbouring regions. Therefore, coordinated measures for prevention, response, and mitigation of their consequences are an important condition for ensuring public safety and the functioning of the economy.

Humanitarian security in cross-border regions consists in preserving cultural heritage and traditions and protecting the population from negative external and internal influences. It implies the absence of ethnic or national discrimination, tolerance, and mutual respect. Without these conditions, it is difficult to establish effective economic and cultural cooperation between border territories.

Criminogenic security within cross-border cooperation is aimed at combating organized crime, illegal drug trafficking, unlawful border crossings, and other criminal activities. The most effective mechanism for addressing these threats is cooperation between the law enforcement agencies of neighbouring states and the coordination of their actions.

Cultural and demographic security is directed toward ensuring the stability of population reproduction in cross-border regions. While policies

to stimulate birth rates are formed at the national level, local authorities are capable of implementing targeted programmes to improve the demographic situation. The creation of new jobs, simplification of border crossings, and development of cross-border cooperation expand the socio-economic opportunities of regions, which has a positive impact on demographic processes.

The legal foundations of cross-border security are defined by international documents of the Council of Europe and the European Union, which outline the key objectives of Euroregions: removing border barriers, equalizing economic and social conditions, developing cooperation among decentralized regions, eliminating infrastructural disparities, building trust, and increasing the effectiveness of interaction.

If cross-border regions include marginalized territories with low birth rates and complex demographic conditions, cross-border cooperation – supported by coordinated national policies and economic stimulation – can become an instrument for their revival.

Processes of Euroregionalization and cross-border cooperation are gaining particular relevance today. For decades, the European community has undertaken efforts to support peripheral and border territories that often face socio-economic marginalization. A significant role in this process has been played by structural funds that financed programmes such as INTERREG III A (2004–2006) and the Czech Republic–Poland Operational Programme (2007–2013). These initiatives contributed to the development of good-neighbourly relations, community integration, joint problem-solving, and enhancement of regional potential.

In the period 2014–2020, new EU funding opportunities emerged for the development of the Polish–Czech border area and for strengthening the role of Euroregions. In the context of the contemporary knowledge-based economy, there is a growing need to improve cooperation formats, implement joint projects, and professionalize cross-border interaction, thereby increasing its long-term effectiveness.

The professionalization of cross-border cooperation and the enhancement of its long-term effectiveness should be based on a clear understanding of the problems, needs, and expectations of all stakeholders involved in the development of border territories, including Euroregion areas [13].

The European Charter of Border and Cross-Border Regions (until 1995 known as the European Charter of Border Regions), adopted by the Council

of Europe on 19 November 1981, emphasizes key aspects of economic, political, and security policy that decisively influence cross-border cooperation. This document was the first to define the concept of 'cross-border cooperation', interpreting it as interaction between neighbouring border regions or cooperation among regional and local authorities, organizations, and institutions representing border areas. The concept encompasses all institutions that contribute to strengthening political, economic, cultural, and security ties between the parties and to concluding agreements of various kinds aimed at developing interregional relations. The implementation of the principles of such cooperation is characterized by two features: the proximity of contacts and a regional or local orientation [15].

Euroregional cooperation serves as an instrument for sustainable economic development and for ensuring the economic security of border territories. However, its impact on the development of specific regions and on cross-border security varies depending on internal and external factors that create preconditions for cooperation.

Scholarly research by foreign and Ukrainian authors has made it possible to systematize the factors that stimulate the development of cross-border cooperation and the functioning of Euroregions. These include geographical, economic, socio-cultural, linguistic, institutional, and international-political factors [7]. The German scholar Robert Knippschild classifies factors into exogenous ones (region size, cooperation experience, needs of particular cities and regions, administrative differences, transnational organizations, regulatory frameworks, linguistic and cultural differences) and endogenous ones (transaction costs, own financial resources, cooperation goals and expectations, participants' competencies, and interaction management). In his view, the key elements are a long-term cooperation perspective, a common strategy, participation of key stakeholders, a coordination office, and initial funding [18].

Ukrainian scholar N.A. Mikula proposes dividing factors into objective ones (the need for joint use of resources, problem-solving, and a unified spatial development policy) and subjective ones (opportunities to enhance socio-economic and environmental development, attract EU funding, improve quality of life, and form a cross-border space) [10, 11, 13].

Other approaches to classifying cross-border cooperation factors also exist, particularly in the business sphere and in other forms of collaboration [4]. However, the issue of the impact of Euroregional cooperation on the cross-border security of a region remains insufficiently studied. Therefore, it

is expedient to systematize the determinants of the direct and indirect influence of Euroregional cooperation on economic development and security of border territories, which makes it possible to forecast risks and threats and to apply appropriate measures to mitigate them or to enhance positive effects.

Cross-border cooperation is not a new phenomenon and existed long before European integration. Its formal definition and legal regulation are associated with the Madrid Convention of 1980, where it was interpreted as cooperation aimed at developing and strengthening good-neighbourly relations between communities or territorial authorities of two or more states through bilateral agreements. Subsequently, with the involvement of both communities and public authorities, cross-border cooperation deepened and became institutionalized in the form of Euroregions.

EU support in the cross-border sphere is implemented through numerous operational programmes and legal instruments, including the European Grouping of Territorial Cooperation (EGTC) [9], which ensures the integration of economic and social activities within the EU. The EGTC grants public-law entities the right to act jointly in member states and to apply for the implementation of measures, thereby increasing partners' autonomy and reducing dependence on political changes in member countries.

Overall, Euroregional cooperation is shaped by internal and external factors manifested at different levels of the economic system: nano (individual), micro (enterprise), and meso (region). These factors directly affect the economic security of a region at the meso-level and indirectly – through the nano and micro levels—as well as the macro level of the state (Fig. 4.1).

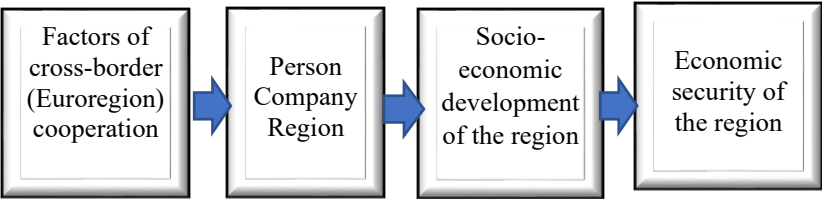


Fig. 4.1. Impact of Euroregional Cooperation on the Economic Security of a Region

Source: author's own elaboration

Considering the various classification approaches to grouping the factors of cross-border cooperation and the specifics of Euroregional interaction, the main groups of factors influencing cross-border security through Euroregional cooperation can be identified as follows:

- financial and economic;
- infrastructure;
- information and communication;
- organizational and institutional;
- integration;
- international and political.

Financial and economic factors include the level of development of Euroregional cooperation, which is a key internal factor of direct mesoscale influence on the region's economic security under cross-border interaction. This group also encompasses the potential for increasing competitiveness. Within Euroregional cooperation and with the support of EU regional policy, centers of competitive activity are shifting to the level of Euroregions, where new hubs of innovation and investment are forming. Euroregions contribute to the development of towns and villages in border areas and enhance their competitiveness. Competitiveness may increase through the development of specific economic sectors, most often tourism, or by improving the overall attractiveness of the region.

At the micro-level, economic security is ensured through the development of small and medium-sized enterprises, and at the nano-level – by creating new jobs. These internal financial and economic factors acquire new properties in the context of cross-border interaction. External factors in this group include international trade, access to resources from EU structural funds and other states (meso-level), opportunities to attract investment and reduce transaction costs (micro-level), as well as ensuring access for civil society organizations to EU funds.

Financial resources attracted within the framework of Euroregional cooperation are primarily directed toward joint projects of border regions, contributing to problem-solving and improving competitiveness. One of the tasks of Euroregions is to ensure participant access to these resources.

Infrastructure factors include the development of transport, border, market, social, and institutional infrastructure, as well as the organization of border trade and border accessibility. Developed infrastructure is key to the effective functioning of the regional economy: it increases the productivity

of agricultural and industrial enterprises and creates conditions for profitability for producers.

Information and communication factors involve the development of personal and family contacts, expansion of the partner network, exchange of innovative experience, information support for Euroregional cooperation participants, and interregional communication. These factors enhance participant activity, reduce border barriers, and encourage the involvement of more actors in cross-border interaction.

Organizational and institutional factors form the foundation for the development of Euroregional cooperation. They include:

- external: cross-border agreements, promotion of cooperation, institutionalization, joint ventures, permits;
- internal: development and coordination of border region development concepts, implementation of management policies, development of civil society.

Institutionalization of Euroregions ensures stability and continuity of cooperation, while cross-border agreements, strategies, and programs create the legal basis for its functioning. Border accessibility is a key factor for economic interaction, facilitating the movement of actors and promoting business activity at the nano- and micro-levels.

Integration factors include the strengthening of interaction between border areas, scientific, cultural, educational, and trade cooperation, conflict mitigation, increased trust, development of civil society, economic convergence, and synergy. These processes support the integration of neighboring regions, although excessive integration can lead to disintegration (as evidenced by Brexit, the situation in Greece, and eastern Ukraine). Disintegration is a reaction to excessive integration and affects economic security.

The regionalization factor manifests in the involvement of regional and local authorities, territorial communities, and associations in decision-making, contributing to the resolution of local problems. International and political factors reflect the subjective determination of the role of Euroregional cooperation at various levels.

Modern understanding of security encompasses all spheres of life and includes threats affecting both internal and external security. It is proposed to distinguish three dimensions of security: subjective, objective, and procedural, which is especially important for assessing security in cross-border regions. The expansion of national security creates new opportunities

for its provision, and national security strategy is based on clearly defined state mission, goals, instruments, and procedures.

The unification of national security issues and the creation of an effective system of its functioning require the development of clear rules and procedures. A universal approach, as applied in the European Union, allows the creation of a system where the same instruments can be effectively used for various types of security activities. For example, armed forces, although intended to counter military aggression, can participate in disaster response, law enforcement support, and citizen assistance in crises.

Many states have revised the modern understanding of national security, which today includes not only measures to counter military aggression. It now encompasses both military and civilian activities aimed at countering threats to the security of the state as a subject of international relations and society. In other words, there are two equal security actors: the state as a political institution and society – the citizens. This implies simplified management rules, creation of a unified national security organizational structure, coordinated use of human and material resources, and simplified procedures for interaction between different activity spheres at the local level.

The expansion of national security is associated with numerous threats, including resource and raw material issues, economic, environmental, and demographic challenges. The interdependence of state and citizen interests, democratization of public life, and the need to balance security with citizens' rights highlight the importance of combining military efforts with measures to ensure the population's quality of life.

Thus, the national security system concerns both the external security of the state – ensuring sovereignty, independence, and territorial integrity – and internal security – protecting citizens, their material well-being, constitutional rights, and national property from threats and natural disasters. National security also defines the framework for activity in cross-border territories and is measured by the achievement of national objectives (Fig. 4.2).

The formation and provision of security in cross-border territories are significantly influenced by the material, technical, social, and cultural foundations of each country. Based on social needs, the state is obliged to create and develop security systems encompassing:

- defense – countering external political and military threats;
- civil protection – minimizing the consequences of natural and anthropogenic hazards, including rescue systems, fire, and flood protection;

- public security – safeguarding the life, health, and property of citizens, protecting principles of social coexistence and legal norms;
- border protection – preventing illegal crossings and the transport of dangerous goods, controlling the spread of infections and hazardous materials;
- information systems security – ensuring uninterrupted operation of management and control systems;
- state and constitutional order protection – countering espionage, terrorism, breaches of state secrets, and crimes against the state.

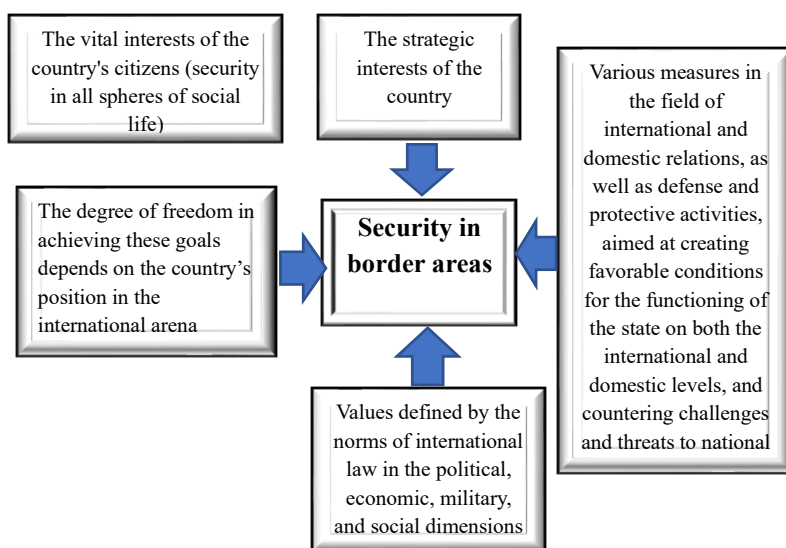


Fig. 4.2. Factors influencing the development of security regulations in border areas

Compiled by the author based on [9]

These systems share common features, highlighting the need for integration into a unified security framework. Such an approach allows effective responses to emergencies by utilizing diverse resources and procedures regulated by state law.

4.2. Border threats and their characteristics

A threat is defined as a situation with a probability of endangering the country. It is crucial to prevent the emergence of challenge – situations that require assessment of the threat level and development of measures for its neutralization.

Modern security understanding goes beyond ensuring state survival and emphasizes the freedom of development. This has led to the emergence of a new scientific discipline – securitology, which studies threats to the existence, development, and civilizational functioning of individuals, social organizations, and states, including cross-border territories.

Scientific security classification distinguishes between:

- by subject criterion – national security, internal and external;
- by object criterion – political, military, economic, social, cultural, ideological, religious, maritime, ecological, informational, legal, food security, etc.

Internal security is part of national security and covers stability and order within the state. External security provides protection against external threats through military structures. In practice, these aspects are not dichotomous but complement each other, particularly in cross-border territories.

Internal security in cross-border regions is understood as a subjective state and process of individual, organizational, and collective activity under real or potentially adverse conditions. It includes the preparation and implementation of measures to predict, neutralize, and manage threats arising in the region and is carried out mainly autonomously under local political guidance. Its goal is to ensure safe existence and development, preserve identified values, and achieve key objectives using all available resources and means.

Other European Union countries also face challenges in defining internal security. This is reflected in the Internal Security Strategy, adopted in March 2010 by the Justice and Home Affairs Council and approved by the European Council. The document defines internal security as a broad and comprehensive concept uniting multiple sectors aimed at responding to serious threats, including natural and anthropogenic disasters (forest fires, earthquakes, floods, storms) directly affecting citizens' lives, safety, and comfort.

Until the mid-1990s, military threats were considered as events in international relations with a high likelihood of restricting or eliminating a state's existence, development, sovereignty, or territorial integrity due to armed violence. This view did not account for the possibility of internal use of military or informational force. A threat is defined as 'a set of internal events that can limit or deprive conditions for the civilizational existence and development of a country and disrupt or lead to the loss of its sovereignty due to armed violence'.

Research on border threats has two main objectives:

1. study mechanisms of interaction between vital interests and threats, forming national interests of the border region as components of overall national interests.
2. identify the balance between the level of protection of vital interests and the effectiveness of countermeasures, on one hand, and the activity of threat realization processes and the severity of their consequences, on the other.

Potential border threats are persistent due to the objective nature of border contradictions. They may manifest as external (objective – natural disasters; subjective – aggressiveness of neighboring states, non-state actors, or individuals) or internal threats (risks, criminality in internal relations). Real threats arising at the border may lead to border conflicts or emergencies requiring the use of appropriate forces and resources.

Threats can be classified into three groups.

1. Those affecting the country's status in the international community – minor but unacceptable for a strong state;
2. Offenses capable of destabilizing the border situation and causing material damage;
3. Threats that can escalate the border situation, cause significant material damage, and impact the overall security of the country.

Additional classification criteria include:

- origin: internal, external; objective economic, social, or political factors;
- degree of impact: highly dangerous, dangerous, less dangerous;
- nature of emergence: domestic policy, foreign states, criminal structures;
- probability of realization: real, potential;
- target object: state, society, individual;
- relative to human activity: objective, subjective;

- object of encroachment: territory;
- predictability: predictable, unpredictable;
- consequences: general, local;
- damage magnitude: catastrophic, significant, moderate.

At specific stages of border activity, security priorities are determined dynamically, depending on the nature and level of threats. The threat system is dynamic, with numerous cause-effect links and feedback loops, which may amplify the consequences of threat realization. This is especially evident under modern state development conditions, characterized by numerous local threats and rapid escalation of crises due to their interaction.

The EU Strategies define the main internal security threats, including:

- terrorism – in any form, disregarding human life and democratic values;
- organized crime – manifesting in various forms across national borders;
- cybercrime – creating global, technical, cross-border, and anonymous threats to information systems;
- transnational crime – significantly affecting citizens' daily lives;
- violence – exacerbates crime damage and harms society;
- natural and anthropogenic disasters – forest fires, earthquakes, floods, storms, droughts, energy failures, and large-scale disruptions of information and communication systems.

Cross-border cooperation is actively developed by municipalities, with its directions, goals, and tools defined by joint regional policy. Globalization processes, creating new challenges and threats, necessitate the development and revision of security guarantees in cross-border territories.

Identification of potential threats in cross-border regions includes:

- external economic threats – shadow economy, factor outflow, excessive foreign investment, dependency on imports. Mitigated through strategic regional planning, foreign investment control, and commodity balance;
- external political threats – territorial separatism, social stratification, ethnic and cultural-linguistic conflicts destabilizing the region;
- food security threats – excessive import of low-quality food. Ensured by supporting domestic producers, innovation, and quality standards;
- energy threats – resource losses due to technical incompatibility of energy systems and low cross-border cooperation. Minimized through

collaboration, international funding, modern technologies, and alternative energy sources;

- environmental threats – pollution of air and soil with toxic substances. Addressed through cross-border programs, EU funds, and environmental security strategies;

- economic threats – regional competition for investments, internal market loss due to imports, inefficient investment use, shadow economy. Addressed via cross-border cooperation and investment in competitive production;

- information threats – low information support and data exchange among cross-border actors, misinformation, and lack of awareness hinder border area development.

4.3. Systemic approach to cross-border security formation

In the modern era of globalization, networks of interdependence among social groups, both formal and informal, increasingly emerge, facilitating communication and mobility while improving neighborly relations. Political will and analysis of potential gains and risks determine adherence to non-intervention and human rights principles.

The modern concept of national security as a comprehensive system of security criteria occupies a leading position and determines the fate of individuals, local communities, and nations due to:

- the significance of individuals and communities as a historically formed collective, based on shared culture, language, religion, territory, and economy;

- the importance of the nation-state as the highest organizational form for achieving national goals with priority on security;

- historical experience – wars, destruction, looting of national wealth, and subjugation.

Euroregions are an organizational form of cross-border cooperation allowing local authorities of border areas, within their competence and with central government consent, to develop comprehensive programs of economic, cultural, and humanitarian interaction. They can implement cross-border economic projects, address employment, infrastructure, and environmental issues.

Research confirms that cooperation within Euroregions effectively enhances social and economic development of territories. Euroregions have

the highest level of institutionalization among all forms of local cross-border cooperation. Currently, there are over 200 Euroregions and more than 30 regional cooperation structures in Europe.

Michael Porter's cluster development concept, formulated in the early 1990s, gained international popularity. Cross-border clusters are unique as their participants operate under different tax, customs, and legal systems but can share enterprises, infrastructure, and operate in cross-border markets. Although borders impose additional barriers to goods, capital, and labor, cross-border clusters gain synergies and become foundations for trade and investment zones.

Integration of government, business, and institutional (scientific, educational, public) efforts promotes investment, accelerates trade, and enhances regional economic efficiency.

Objectives of cross-border cooperation:

- convergence and standard of living alignment – eliminating disparities between adjacent border regions and reducing borders as barriers;
- structural transformation – changing regional socio-economic development models, efficient use of grants, and subsidiarity development;
- regional competitiveness and employment – supporting economic changes in industry, urban and rural areas, increasing competitiveness and attractiveness.

Organizational features of Euroregions:

- Euroregions do not create an additional management level; they facilitate interaction of local, regional, state authorities, and private structures on both sides of the border;
 - cooperation programs are implemented under national legislation of each country;
 - local authorities make autonomous decisions, while central ministries coordinate activities;
 - the 1996 Karlsruhe Agreement allows regional and local authorities to independently conclude agreements with border partners, creating a legal framework for cross-border cooperation.
- Functions and significance of cross-border cooperation:
- improving living conditions of border populations;
 - creating regional network communities for resource sharing and coordination;
 - participation in EU projects;

- stimulating private sector and civic initiatives, especially in socially and economically asymmetric regions;
- supporting European integration and development of municipal partnership networks.

- EU regional policy principles implemented in Euroregions:
 - general – subsidiarity, flexibility, coordination;
 - organizational – programming, partnership, stability, consistency;
 - financial – concentration, additivity, complementarity;
 - program management – monitoring, evaluation, financial control.

Thus, Euroregions are a priority form of cross-border cooperation, promoting integration, economic development, and improved social conditions in border regions.

A systemic approach to Euroregion security (Fig. 4.3) involves comprehensive analysis of the roles and interconnections of systemic components and decision-making factors, adhering to principles such as:

- polycentricity – the Euroregion's environment is considered a complex analytical object. Interaction of influence centers and actors defines security processes;

- hierarchy – management goals are structured hierarchically: EU-wide, national, regional, and Euroregion goals, ensuring strong linkage between local and supranational security policies;

- entropy – security measures are structured according to the uncertainty of available or forecasted information, especially for assessing threats to national interests;

- optimality – resource costs and security results are evaluated through multi-criteria analysis to select the best course of action;

- adequacy of purpose and outcome – ensuring alignment between objectives and results. For each alternative solution, the potential level of protection of national interests is assessed in the event of its practical implementation;

- principle of adequacy of managerial decisions to the threat level. Only those alternatives that correspond to the level of threats are considered. Insufficient response may lead to increased risks to national interests;

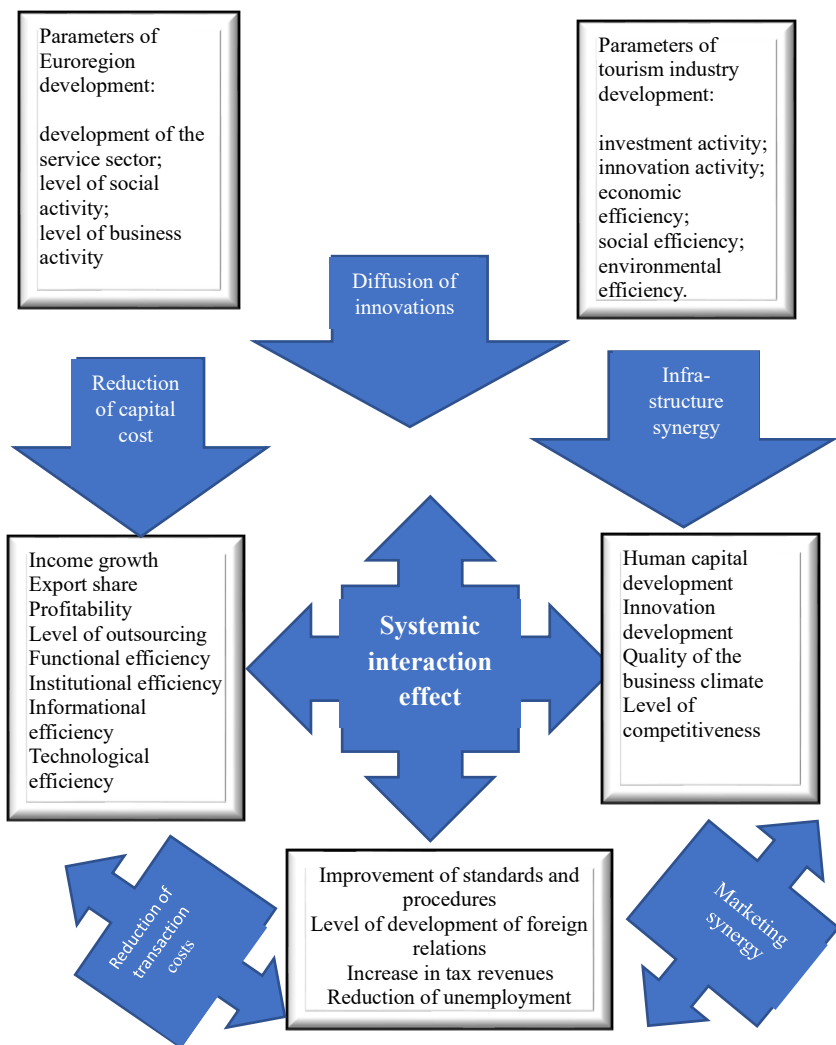


Fig. 4.3. Parameters of network interaction in the process of forming Euroregional security

Source: [17]

– principle of multiplicity (variety) of options
Decision-making is viewed as selecting from a set of alternatives, which requires the availability of a sufficient number of options.

– The sequence of actions is determined by situational conditions, particularly the available time and resources.

– Considering the institutional and legal aspects of the decision-making model should:

– systematize information from environmental analysis to decision implementation;

– reflect power relations, national values, and interests;

– be supported by legal mechanisms of the political system.

Thus, the systemic approach enables the provision of a comprehensive, adequate, and adaptive security system for the Euroregion, taking into account the interconnection between different management levels and the complexity of external and internal operating conditions.

References

1. Babets, I. H. (2014). Information security of Ukraine's interregional cooperation: institutional aspect. *Social and Economic Problems of the Modern Period of Ukraine*, (3), 518–527.

2. Volkova, N. (2023). Cross-border cooperation of Ukraine with EU countries under the conditions of the Russian-Ukrainian war. *Economics and Society*, (48). <https://doi.org/10.32782/2524-0072/2023-48-52>

3. Hoblyk, V. V. (2013). Prospects for the development of cross-border clusters on the border of Ukraine with the European Union. *Effective Economy*, (3). Available at: http://nbuv.gov.ua/UJRN/efek_2013_3_7

4. Homolska, N. I., & Chertoryzhskiy, V. M. (2010). New forms of international economic integration – prospects for cross-border cooperation. *Scientific Bulletin of NLTU of Ukraine*, 20.5, 173–177.

5. Economic Security: Textbook/Ed. Z.S. Varnaliya. Kyiv: Znannya, 2009. 647 p.

6. European Framework Convention on Cross-border Cooperation between Territorial Communities or Authorities. Available at: <https://ips.ligazakon.net/document/MU80K15U>

7. Derbak, V. I. (2022). Cross-border cooperation: theoretical and methodological aspect. *Scientific Bulletin of Uzhhorod University. Series: Law*, 71, 342–347.

8. Kalat, Ya. Ya., & Demedyuk, O. P. (2017). Prospects for the development of institutionalized forms of cross-border cooperation in Ukraine. *Social and Economic Problems of the Modern Period of Ukraine*, (5), 92–97.
9. Malyarenko, T. A. (2009). Economic Security: educational-methodical manual. Donetsk: DonDUU, 129 p.
10. Mikula, N. A. (2008). Strategy of formation and support of cross-border clusters. In E. I. Boiko (Ed.), *Clusters and competitiveness of border regions: collection of scientific papers* (Vol. 3(71), pp. 129–141). Lviv: NAS of Ukraine, Institute of Regional Studies.
11. Mikula, N. A., & Zasadko, V. V. (n.d.). On improving financing mechanisms for Ukrainian-Polish cross-border cooperation projects: analytical note [Electronic resource]. National Institute for Strategic Studies. Available at: <http://www.niss.gov.ua/articles/1064/>
12. Artyomov, I. V., et al. (Ed.). Models and mechanisms for regulating Euroregional cooperation in Ukraine: Monograph. Eds.: I.V. Artyomov, O.M. Vashchuk, O.M. Rudenko.
13. Mikula, N., & Hoblyk, V. (2013). Creation of cross-border industrial zones and technology parks as a means of activating foreign economic relations in cross-border regions. In *Problems of development of foreign economic relations and attracting foreign investments: regional aspect* (Vol. 1, pp. 227–231).
14. Mikula, N. A., & Tolkowanov, V. V. (2011). *Cross-border cooperation* (manual). Kyiv: Kramar, 259 p.
15. Tikhomirova, E. B. (2010). Information support of cross-border cooperation: Polish experience. *Scientific Bulletin of Volyn National University named after Lesya Ukrainka*, (26), 18–24.
16. Khymynets, V. V., Holovka, A. A., & Mirus, O. I. (2021). Cross-border cooperation as a tool for local and regional development: analytical report. Kyiv: NISD, 47 p.
17. Tkach, S. M. (n.d.). Economic security system: regional aspect [Electronic resource]. Available at: http://www.rusnauka.com/4_SND_2012/Economics/4_100344.doc.htm
18. Knippschild, R. (2007). *Cross-border cooperation: design and management of cooperation in spatial development in the German-Polish-Czech borderlands* [Electronic resource]. Access: <http://goo.gl/Ht0Ip8>
19. Okunyovska, Yu. V. (2022). Cross-border cooperation with Ukraine in the conditions of war. *Bulletin of DonNU named after Vasyl Stus, Series: Political Sciences*, (7), 70–74.

20. Hakli, J. Cross-border identities in the new Europe: Ghost of the past or sign-post to the next millennium. Available at: <http://www.may.ie/staff/dpringle/igu/hakli.pdf>

Chapter 5

Global business risks and directions for their minimization

(O. Havryliuk)

In the modern interconnected world, the business landscape is constantly changing, and with it the complexity of risks faced by countries and companies is growing. From geopolitical instability and trade wars to cyber threats, supply chain disruptions, and climate change, every global player operates in an environment where potential dangers can quickly turn into serious financial losses or even lead to collapse. Ignoring these risks is no longer an option; they require proactive management and a comprehensive strategic approach. Success in maintaining competitive positions and ensuring sustainable operations directly depends on the ability not only to react to crises and risky phenomena but to anticipate them and embed resilience into the operational model.

This chapter analyzes the key global business risks that dominate the 2020s and develops effective strategies for their minimization. It also considers strategies and tools for building adaptive risk management systems, with a focus on transforming potential threats into manageable challenges, thereby ensuring the viability and protection of business on the global stage. The tasks of the chapter include:

- identification of the main global risks that will determine virtually all spheres of societal life in the near future;
- outlining their hypothetical consequences and strategies for minimization and increasing resilience;
- highlighting the main business risks of Ukraine in wartime, with justification of approaches to their resolution;
- formulation of recommendations and application of tools, including artificial intelligence, for minimizing global threats.

5.1. Identification of the main global business risks

Identifying the main global business risks is critically important for strategic planning and ensuring resilience in the modern interconnected world. Risks ranging from geopolitical instability to rapid technological changes are constantly evolving, presenting both significant threats and new opportunities for companies operating in the international environment.

The landscape of global business risks is dynamic and multifaceted. While specific issues change annually, several key categories of threats consistently dominate the list of risks that companies must effectively manage. These include:

1. Geopolitical instability, which encompasses international conflicts, trade wars, sanctions, political unrest, and sudden changes in state policy. Such events can disrupt supply chains, close markets, and sharply increase operational uncertainty and costs.

2. Economic volatility. Risks in this category include global recessions, high inflation, rising interest rates, currency fluctuations, and sovereign debt crises. These factors directly affect consumer demand, the cost of financing, and the profitability of investments.

3. Cyber threats and data security. With growing digitalization, the risk of sophisticated cyberattacks, data breaches, and ransomware becomes paramount. A successful attack can lead to significant financial losses, reputational damage, and regulatory fines.

4. Climate change and environmental risks. This category covers both the direct impact of extreme weather events and the long-term consequences of transitioning to a low-carbon economy, new environmental regulations, and resource shortages.

5. Production disruptions and supply chain interruptions. Events such as natural disasters, pandemics, or geopolitical conflicts can seriously interrupt the flow of goods and raw materials, causing production delays and inventory shortages.

6. Regulatory and legal changes. Businesses face risks from constantly changing compliance requirements related to data privacy, environmental standards, antitrust legislation, and international tax policy, which increase the complexity and cost of global operations.

Understanding and prioritizing these risks allows companies to develop robust mitigation strategies, ranging from diversifying supply chains and

investing in cybersecurity to creating financial reserves and conducting scenario planning.

There are global entities for identifying and warning about risks whose recommendations many companies heed. They identify risks that generally coincide, although ranked somewhat differently.

World Economic Forum – a Swiss non-governmental non-profit organization best known for organizing annual meetings in Davos. The meetings bring together leading business executives, political leaders, prominent thinkers, and journalists.

Marsh & McLennan Companies, Inc. – a global professional services firm headquartered in New York. It specializes in risk management, reinsurance services, investment consulting, and management consulting. It helps clients anticipate risks threatening their operations, quantitatively measure and manage these risks, transform them into opportunities, and uncover new business development prospects.

Allianz SE – a German insurance company and one of the largest in the world, classified as systemically important to the global economy. Since its founding in 1890 it has operated on all major financial markets worldwide.

Control Risks – a global consulting firm specializing in risks related to politics, security, and integrity. Founded in 1975, with headquarters in London.

J.S. Held – a global consulting firm that combines technical, scientific, financial, and strategic expertise to advise clients seeking to realize value and reduce risks.

Everstream – a US-based company that serves business clients by providing AI-driven supply chain risk intelligence and resilience solutions, including advanced monitoring tools and expert support.

The World Economic Forum in its annual Global Risks Report 2025 lists among current global risks: interstate armed conflicts, extreme weather events, geoeconomic confrontation, disinformation, societal polarization, economic downturn, critical changes in Earth's systems, lack of economic opportunity/unemployment, erosion of civil liberties, and inequality. However, institutions whose primary competence is tracking and preventing business-specific risks apply somewhat different approaches and criteria, which are taken into account in this chapter.

In the Allianz Risk Barometer, cyber incidents (cybercrime, IT network and service failures, deployment of malicious software such as ransomware, theft and data leaks) are ranked as the main global business risk in 2025 – the

fourth year in a row that cyber incidents top the list of leading risks. Everstream ranks them third. Ten years ago, this factor was only in 8th place worldwide. In 2025, cyber incidents are attributed to the highest risk category for Europe, North and South America, Africa, and the Middle East – overall for 20 countries: Argentina, Australia, Belgium, Brazil, Colombia, France, Germany, India, Italy, Kenya, Mauritius, Morocco, Nigeria, the Philippines, Portugal, South Africa, Switzerland, Uganda, the United Kingdom, and the USA. As can be seen, the Asian region has so far been less represented among the highest-risk countries in this context. Cyber incidents also pose the highest risk for eight sectors, such as aviation, the chemical industry, entertainment, financial services, media, and professional services. Cyber is also considered the highest risk for large, medium, and small companies. Countries that have suffered the largest losses from cyberattacks (including ransomware, data breach reports, and the overall number of incidents) are predominantly concentrated in North America and Europe – the USA, Israel, the United Kingdom, France, and Australia.

The negative consequences of cyberattacks include:

- disabling critically important state and business systems (websites, electronic government services for the population and business, online stores, accounts of key managers, etc.);

- loss of personal, corporate, and confidential information;

- theft of personal and financial data, leading to unauthorized withdrawals of funds;

- damage to the company's business reputation and resulting loss of clients;

- material costs for eliminating the consequences of cyber incidents.

Data breaches, attacks on critical infrastructure or physical assets, and the increase in ransomware attacks are causing growing cyber concerns. This is related to the high level of digitalization, financial attractiveness, and geopolitical factors.

Several key trends currently drive modern cyber activity. Hackers are increasingly targeting information technologies and physical supply chains, launching mass cyberattacks and finding new ways to extort money from large and small companies. Information technology (IT) is a broad field that encompasses the use of computers, software, networks, databases, and other equipment and technologies to create, process, store, protect, and exchange all kinds of electronic data and information. IT is the foundation of the modern economy and society, ensuring the functioning of almost all

organizations and spheres of life. IT includes: hardware – physical devices such as computers (personal PCs, servers), mobile devices, network equipment (routers, switches), printers, and more; software – intangible programs and instructions that make hardware perform specific tasks, including operating systems (Windows, macOS), application programs (Microsoft Office, Photoshop), and specialized business systems (CRM, ERP); networks and communications – systems that allow computers and devices to exchange data, including local area networks (LAN), wide area networks (WAN), and, most importantly, the Internet. The main functions of IT include process automation, data storage and management, simplified communications, and security – protection of information assets from unauthorized access, cyberattacks, and data loss (cybersecurity).

More than half of all cybercrimes are committed with the aim of stealing information, primarily personal data of legal entities and individuals. Individuals most often risk their accounts and bank card data. However, current cyber threats go far beyond hacker attacks and data leaks. The constantly growing capabilities of cybercriminals force companies to pay close attention to risks facing their critical infrastructure, including IT, water, and electricity supply systems.

Information leakage consistently poses a danger. Digital technologies can significantly increase the risks of information leakage, especially regarding the storage of personal data and work with confidential information. Ensuring an adequate level of security, in turn, can significantly increase the cost of digitalization. Therefore, these additional risks and their possible consequences, which can cause direct and indirect damage to the company's reputation, its clients and counterparties, and the business as a whole, should be carefully weighed. To avoid these consequences, many opportunities for cybercriminals should be eliminated, and the following measures should be taken, including:

- installation of up-to-date cybersecurity systems and data traffic control, the use of only licensed software, and its timely updating;
- regular cyber audits to check the vulnerability of the cybersecurity system, identify, and fix weak or vulnerable spots;
- transferring all possible data to the cloud with multiple backups in different regions or even countries – especially relevant for Ukrainian companies in wartime conditions;
- monitoring new threats and regularly adapting protection policies;

- informing relevant state authorities in case of suspicion of potential cyber incidents.

Overcoming cybercrime is hindered by a global shortage of personnel in cybersecurity – over 4 million people – with demand growing roughly twice as fast as the supply of qualified professionals. Currently, there are serious problems with hiring professional cybersecurity engineers, and without qualified personnel it is quite difficult to predict and prevent incidents, which can lead to increased losses in the future.

To combat cyber threats, enterprises can and should apply a proactive approach by identifying the most important assets and vulnerable points of the information system and then deploying appropriate software for threat detection and monitoring both at the network perimeter and at endpoints. A proactive approach is a style of thinking and behavior in which the subject acts ahead of events, anticipating possible problems and opportunities rather than merely reacting to circumstances. The main features of a proactive approach are based on the following elements:

- anticipation – analysis of hypothetical risks and opportunities and identification of options for action in advance;

- initiative – independent decision-making and searching for solutions without external pressure;

- focus on possible vectors of business strategy transformation;

- flexibility – adaptation to changes and justification of new strategies to achieve goals.

A proactive approach to minimizing or eliminating the consequences of rapid changes in the modern business environment makes it possible to control the situation rather than simply adapt to it and involves the following steps:

1. Analysis of trends through regular monitoring of market trends, technological innovations, and changes in consumer behavior using analytics, industry reports, and platforms like Google Trends or Statista.

2. Building a flexible strategy by developing an adaptive business plan with several alternative scenarios (optimistic, pessimistic, baseline) and conducting quarterly reviews.

3. Diversification of revenue sources, customer base, and markets, including reducing dependence on a single supplier.

4. Investment in technologies through process automation and the implementation of digital tools (CRM, ERP, AI-based analytics) for a prompt response to changes.

5. Staff training through regular workshops to master new skills, especially in the digital sphere.

6. Ensuring the availability of a financial buffer and a reserve fund to cover expenses in case of economic downturns or unexpected costs.

7. Strengthening the network of contacts with partners, clients, and industry experts, which allows gaining insights and support.

8. Monitoring competitors – tracking their actions, innovations, and strategies for timely adaptation.

9. Legal readiness – tracking changes in legislation, taxes, and regulations that can impact the business.

10. Customer orientation and product centrism – continuous collection of feedback from customers in order to adapt products and services to their needs.

Among the highest business risks over the last ten years are production disruptions, which pose a particular threat to the Asia-Pacific region and twelve countries – Austria, Canada, China, Hong Kong, Indonesia, Malaysia, Mexico, the Kingdom of the Netherlands, the Philippines, Singapore, the Republic of Korea, and Sweden. This is also the highest risk for eleven sectors, such as consumer goods manufacturing, leisure and entertainment, food and beverage production, heavy industry, hospitality, the automotive industry, the oil and gas sector, energy and utilities, renewable energy, and transport and logistics. The most important tools for minimizing these risks that companies resort to include measures to secure their supply chains and enhance their resilience, notably through diversification and increasing the number of suppliers, geographical expansion of supplier networks – as a response to unstable and unpredictable geopolitical trends – and improving business continuity management.

Shortage of qualified specialists – recruiting and retaining qualified personnel – is another acute problem: 75% of companies worldwide experience difficulties due to talent shortages and hiring challenges [6; 7]. Employers in the healthcare and industrial sectors suffer from a shortage of specialists with IT and data processing skills. Moreover, not only employees but also owners of small and medium-sized businesses often prove to be unqualified. The analysis made it possible to generalize the reasons for the incompetence of the management staff as follows:

1. Lack of understanding of the market in which the company operates, including its target audience (with attempts to generalize it), and ignorance of competitors and their advantages.

2. Absence of a system for attracting and retaining clients, as a result of which owners have no idea how to build a base of loyal clients, leading to intensive growth of the so-called ‘base of former clients’.

3. Inefficiency of the organizational structure. Often, owners do not understand the formula for company growth; consequently, unprofessional employees work in the business, staff numbers are inflated, and responsibilities are scattered due to poorly distributed functions, making it impossible to identify the responsible person.

4. Absence of a staff training system. Most often, the owner expects that a new experienced employee will instantly integrate into the work process, but in practice onboarding can take several months.

5. Inefficiency of managers, as a result of which appointments to management positions occur without building their management culture. The problem of many managers lies in the lack of knowledge regarding full-fledged leadership, which determines the inefficiency of internal processes.

6. Inefficiency in financial management, including cases when the owner’s finances are mixed with business finances and key management reports (balance sheet, P&L, cash flow, etc.) are absent.

7. Absence of long-term planning, with the owner’s vision often not extending beyond one or two months of operations.

8. Excessive dependence of the company’s activities on the owner, when all key operations are concentrated in their hands.

In summary, a key underlying cause of instability or collapse in many modern businesses is the insufficient managerial competence of their owners. A typical situation arises when owners do not know what their business should ideally look like and, paradoxically, are convinced that business education is unnecessary.

Climate change has entered the top five risks, taking 5th place (7th in 2024) – the highest position in the history of the Allianz Risk Barometer. The closely related risk of natural catastrophes is ranked 3rd. Critical changes in Earth’s systems concern significant transformations in natural processes and ecosystems, mostly caused by anthropogenic activity: climate change, loss of biodiversity, deforestation, ocean acidification, and planetary pollution.

Business awareness of the need to implement measures to increase climate resilience is growing, driven by the rise in companies’ costs for complying with regulatory requirements on the disclosure of physical climate risks, as well as operational disruptions due to more extreme weather events

and ecosystem degradation. Three main consequences of climate change that companies fear the most can be highlighted:

- acute physical impact (e.g., damage to production facilities due to extreme weather conditions);
- impact on business interruptions (e.g., bottlenecks in supply chains, logistics disruptions due to extreme weather events);
- environmental impact (e.g., extreme temperatures, resource shortages, loss of biodiversity).

To mitigate the direct impact of climate change, companies typically use at least three strategies, namely: adaptation or increasing insurance coverage (including alternative risk transfer); implementing business models that reduce carbon emissions (e.g., recycling and waste reduction, encouraging eco-friendly transport, developing more resilient supply chains); and creating contingency plans for climate-related unforeseen circumstances (e.g., response and recovery measures, assessment of critical systems and resources).

A relatively new addition to the biggest global risks is the impact of risks arising from new technologies, such as artificial intelligence (AI).

The use of artificial intelligence remains an underexplored domain and can bring both benefits and dangers to the business sphere. Practice has already shown that improvements in newer versions do not automatically translate into increased safety for either business or ordinary citizens. For instance, the release of GPT-4 (March 2023) was aimed not only at optimizing the functionality of ChatGPT but also at reducing the likelihood of producing potentially harmful results. However, reality has demonstrated the opposite in some respects: at seminars of the European Union's law enforcement agency – the European Police Office (Europol) – when various cases of criminal use of the previous version GPT-3.5 were examined, it was shown that all of them work in GPT-4 and in some cases have become even more advanced. In response to a wide range of prompts, ChatGPT provides users with ready-to-use professional information: even without basic knowledge about specific spheres of criminality, a potential offender can receive from artificial intelligence a wide range of possible unlawful activities, from building penetration to terrorism, cybercrime, and sexual violence. Based on this, it is already clear how diverse and potentially dangerous AI can be in the hands of malicious actors. Europol's report 'The Impact of Large Language Models on Law Enforcement' (March 27, 2023)

contains a warning that the rapid development of generative AI can contribute to the activities of online scammers and cybercriminals [9, p. 2].

Thus, artificial intelligence cannot be considered a panacea for solving all problems of entrepreneurship security. First, it can be used with malicious intent; second, the probability of AI systems transitioning into an uncontrollable state cannot be excluded. Concerns about the latter were expressed by Elon Musk and a number of prominent business leaders on March 29, 2023; they called for a temporary halt to its development.

5.2. Modern risks and problems of Ukraine

Global business risks are particularly acutely extrapolated to the realities of Ukraine, which is fighting Russian aggression. The ongoing war obliges not only to concentrate efforts on victory over the enemy but also to anticipate paths for the fastest possible economic recovery based on effective strategies. The tasks of this section include highlighting the following issues:

- specification of strategic directions for securing business during wartime;
- formulation of recommendations for minimizing the negative consequences of the war for business.

According to data as of February 2025, Russia's war has caused 176 billion USD in damage to Ukraine's infrastructure. The residential sector has suffered the most, with damages estimated at 60 billion USD. In total, 236,000 residential buildings have been damaged or destroyed, including 209,000 private homes, 27,000 apartment buildings, and 600 dormitories. Among the most affected regions are Donetsk, Kharkiv, Luhansk, Kyiv, Chernihiv, and Kherson oblasts. As of February 25, 2025, the total estimated cost of reconstruction and recovery in Ukraine amounted to 524 billion USD (506 billion EUR).

Conducting business during the war is an extremely challenging but realistic task and requires securing the functioning of assets and personnel. However, ongoing attacks on Ukrainian infrastructure can significantly slow down economic activity, necessitating enhanced security and risk minimization. After the start of the war, new realities and risks have emerged, including:

- migration of people and the complexity of their return;
- absence of personal safety anywhere;
- risks of loss of property and personnel;

- increase in the number of enterprises unable to fulfill their obligations.

Adding to this list radical changes to legislation creates a multi-risk situation for every enterprise, requiring the resolution and minimization of real risks and threats.

First and foremost, personnel and property (assets) need to be secured. Whenever possible, staff reductions should be avoided, as preserving personnel is a critically important step: after victory, experienced and proven staff will be needed for recovery, and there is a high risk of their shortage. An important step is to establish constant communication with employees, for example through groups in messengers or organizing work on platforms like Microsoft Teams. Every enterprise also needs to retain a critical number of personnel for operations, which requires addressing the procedure for reserving key employees.

The next step is transitioning to electronic document management – a process that is inevitable in any case – through which corporate documents will be accessible at any time to persons with access rights. Such documents will not disappear, and it will be impossible to physically destroy or steal them.

Business risks inherent to wartime, such as non-fulfillment of obligations and, accordingly, the reliability of counterparties, become particularly relevant. Business owners should be on guard when a previously reliable counterparty may fail to fulfill contract terms, necessitating measures to minimize risks in this area, namely:

- renegotiating contracts by adding conditions for resolving problem situations;

- being more cautious with supplies on deferred payment terms;

- conducting repeated checks of the reliability of existing clients, as in transitional and unpredictable conditions they may face serious problems;

- verifying the availability of signed and extended contracts and other primary documents, as they will be urgently needed for court appeals.

Under martial law, legislation for business changes almost daily, and after ensuring the physical safety of employees and the enterprise's property, the next task is to organize legal security. Although in recent years the issue of raiding has become less acute, despite restrictions on access to most registers under martial law, the risk of illegal raider seizure of property (entering changes to state registers regarding the owner, director, location of property, or registration of ownership rights through forgery of documents and information) remains high. Risks of raider seizure can be minimized by

properly drafted statutory documents of the enterprise. Necessary provisions for preserving the institution include: defining the rights and duties of its governing bodies – the director, supervisory board, and general meetings – depending on the form of registration; procedures for holding general meetings of owners and notifying participants of upcoming meetings, as well as proper registration of minutes of general meetings; the mechanism for changing the composition of owners; introduction of a reservation system for concluding agreements on the alienation of shares; restrictions on the director's ability to enter into legally significant transactions and sign contracts depending on their value, etc., all in accordance with the Law of Ukraine “On Amendments to Certain Laws of Ukraine Regarding Improvement of the Mechanism to Counter Raiding” No. 2255-IX of May 12, 2022.

One of the most acute issues is the registration of rights to all assets. During business operations, managers do not always pay attention to obtaining documents for equipment and registering trademarks. However, the absence of such documents will make it impossible to prove rights to these assets. This primarily concerns the preparation of current procedural acts documenting the withdrawal of assets from the company's ownership. This can happen for various reasons: damage after an explosion, abandonment in occupied territory, or looting. On the other hand, property may be transferred for the needs of the Armed Forces of Ukraine. In each case, a proper documentary trail is required, as in the future, without confirming documents, it will be impossible to claim compensation or return of property.

Currently, there is also danger associated with reputational risks: under wartime conditions, a new practice is gaining momentum – a new way of eliminating competitors. Initially, a PR campaign is conducted, most often through “leak” Telegram news channels, where a certain company is labeled a traitor working for the occupiers. Usually, not every business can survive such a blow and refute the slander; moreover, subsequently, “unexpectedly”, representatives of competent authorities often visit the enterprise with searches, after which there is a high risk of asset deprivation. If a company appears in such news feeds, it is necessary to immediately contact PR specialists and lawyers specializing in criminal cases.

Russia's war against Ukraine and the associated physical losses, damage or seizure of property and cargo, injury or death of employees, etc., are primary risks. Some enterprises, such as those in metallurgy and the mining industry, agriculture, and logistics, especially near the front line, although

located in high-risk zones, cannot be relocated, and protection from military risks becomes a priority for entrepreneurs. Therefore, in addition to the above directions for security, insurance of political (military) risks, accidents, and business interruption losses should be considered. On the one hand, as a result of Russia's invasion, the vast majority of insurance service providers have suspended their operations in Ukraine; on the other, several institutions still offer insurance options, including MIGA (World Bank Group), DFC (USA), UKEF (United Kingdom), KUKE (Poland), SACE (Italy), and others. Their services can realistically be utilized. Ideally, companies should have backup equipment and stocks of raw materials, fuel, and materials, monitor the development of the security situation in Ukraine, and implement cybersecurity measures.

Finally, the issue of minimizing one of the main global business risks – cyber threats – requires special attention. In 2024, Ukraine experienced a significant increase in cyberattacks from Russia. According to the State Service of Special Communications and Information Protection of Ukraine (State Special Communications Service) and the government response team CERT-UA, the number of registered cyber incidents increased by 69.8% compared to 2023 – from 2,541 to 4,315 incidents, including over 3 million security events. In the second half of 2024, 2,576 incidents were recorded – an increase of 48% compared to the first half of the year.

Countering cyberattacks is feasible through strengthening cybersecurity and using artificial intelligence (AI). AI can process large volumes of data and identify trends and patterns that may indicate future changes in the economic and political situation. Using publicly available and specialized data with artificial intelligence allows obtaining critically important information for the functioning of entrepreneurial structures, as well as applying innovative technologies and tools in the recovery of affected cities.

AI is already learning lessons from Russia's war in Ukraine. In March 2022, the Ministry of Defense of Ukraine began using the facial recognition system of the US-based ClearView AI company, which has access to 10 billion photos from social networks, thus enabling the probable identification of the faces of deceased Russian soldiers and notification of their families about their death. Currently, the possibility of implementing ClearView AI in courts, healthcare institutions, and customs is being studied.

Based on this, it is possible to formulate directions for minimizing risks of property and personnel loss and securing entrepreneurship in wartime conditions using AI:

1. Development of a monitoring system that tracks changes in the political and economic conjuncture and warns entrepreneurs about hypothetical risks and threats, facilitating more informed decisions on investments and development strategies.

2. Forecasting future market trends with preemptive responses. Analysis of economic dynamics, production, consumption, export, and import data will allow identifying risks and structural changes in the economy. For example, AI can identify strategically important goods and assess risks in their production or supply.

3. Optimization of business processes using robotic systems, which can significantly reduce the number of errors in decision-making.

4. Use of data protection and cybersecurity systems, which help prevent leakage of confidential information, detect emerging cyberattacks or unusual personnel activity aimed at leaking confidential information, identify security breaches, and block or restrict access to confidential information through the use of facial recognition algorithms and other user authentication technologies.

5. Cooperation with national and regional government authorities, which makes it possible to obtain information on changes in the political and economic conjuncture, track changes in government policy, assess new regulatory norms and laws to anticipate possible risks and promptly make informed decisions, as well as receive protection from state authorities, including holding violators accountable and appealing to court for compensation of damages. In the event of potential cyber incidents, relevant state structures must be immediately informed. Transferring all possible data to cloud services and storing multiple backups in different regions or even countries is especially relevant for Ukrainian companies in wartime conditions.

6. Development of anti-crisis plans and strategies based on an algorithm for preserving business in case of threats and catastrophic events.

The implementation and development of digital technologies in business organizations, regardless of their form of ownership and subordination, are accompanied by an intensification and diversification of threats and real consequences of cyberattacks. During wartime, every enterprise must operate in a heightened readiness mode and pre-assess the vulnerability of its critical services to cyber incidents and technological failures to prevent negative consequences from malicious attacks. Strengthening cybersecurity will contribute to minimizing the negative

consequences of such incidents. Improving the legal and regulatory framework for entrepreneurship cybersecurity is also on the agenda. This area requires legal support, as the regulation of cybersecurity in Ukraine is fragmented: norms regulating it are scattered across many laws and subordinate acts; in the event of a cyber incident, it is extremely difficult for a business owner to independently find the necessary information for protection.

The outlined list of strategic directions is far from complete, but taking them into account will contribute to securing business. Identification of global business risks has transformed from a periodic exercise into a continuous strategic imperative. In a world where the interconnection of technologies (for example, the uncontrolled development of AI) and geopolitical forces can cause instantaneous and catastrophic disruptions, business success depends on the ability not only to manage known threats but also to anticipate the “unpredictable” and quickly adapt to it. True resilience requires not just risk minimization but the integration of flexibility and security into the very foundation of the business model.

References

1. The Global Risks Report 2025. P. 6. Available at: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf
2. Allianz Risk Barometer. Identifying the major business risks for 2025. Available at: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf>
3. Talking Supply Chain Risks to Gain Competitive Edge. 2025. Available at: <https://mail.google.com/mail/u/0/#trash/FMfcgzQZVKFbLXksvfPsqexzMDcrgLrS>
4. Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About! 20 January 2025. Available at: <https://www.em-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about>
5. Cost of a Data Breach Report 2025. Available at: <https://www.ibm.com/reports/data-breach>

6. Global Talent Shortage 2025. Available at: <https://go.manpowergroup.com/talent-shortage>

7. Talent shortage insights: Recruitment solutions for 2025. Available at: <https://www.manatal.com/blog/talent-shortage>

8. Europol sounds alarm about criminal use of ChatGPT, sees grim outlook. AVAILABLE AT: <https://www.reuters.com/technology/europol-sounds-alarm-about-criminal-use-chatgpt-sees-grim-outlook-2023-03-27/>.

9. Europol. ChatGPT. The impact of Large Language Models on Law Enforcement. Available at: <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>

10. Elon Musk among experts urging a halt to AI training. Available at: <https://www.bbc.com/news/technology-65110030>.

11. Updated damage assessment finds \$524 billion needed for recovery in Ukraine over next decade. February 25, 2025. Available at: https://www.undp.org/ukraine/press-releases/updated-damage-assessment-finds-524-billion-needed-recovery-ukraine-over-next-decade?utm_source=chatgpt.com

12. Війна Росії завдала інфраструктурі України збитків на \$170 млрд. Available at: <https://www.kyivpost.com/uk/post/47343>

13. Закон України «Про внесення змін до деяких законів України щодо удосконалення механізму протидії рейдерству» № 2255-IX від 12.05.2022. Available at: <https://zakon.rada.gov.ua/laws/show/2255-20#Text>.

14. Mitigating risks for foreign investors in Ukraine. December 4, 2023. Available at: <https://dlf.ua/en/mitigating-risks-for-foreign-investors-in-ukraine/>

15. Державна служба спеціального зв'язку та захисту інформації України. Аналітичні матеріали Держспецзв'язку. Available at: <https://www.cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku>

16. Міноборони почало використовувати американську систему розпізнавання обличь. Available at: <https://epravda.com.ua/news/2022/03/14/683964/>

Chapter 6
Strategic aspects of energy and environmental safety
management
(A. Dychko, Y. Minaieva, A. Hlukhonets)

The energy and environmental safety of Ukraine is determined by the influence of internal technical, technological, and informational factors, as well as external natural and military factors. Risk forecasting is based on statistical data on the possible causes of man-made and environmental disasters, as well as various models of functioning, behavior, and development of events, based on different initial data and criteria. However, reliable statistical data can only be obtained if there is information on a significant number of cases with clearly defined conditions for the emergence of environmental or energy disasters. In the case of unique disasters, there is no statistics, which makes predicting the risks of their occurrence quite a difficult problem, since even failure statistics is based on considerations of average operating conditions, average external and internal factors, etc. [1]. Statistics is based on assumptions about the 'average state' of technical and software resources, staff training, external conditions, etc.

The aim of the study is to identify the key aspects of risk-oriented management of energy and environmental safety.

6.1. Strategic aspects of energy and environmental safety

The functioning of industrial enterprises is often associated with permanent environmental pollution (corpuscular, chemical, thermal, radiation, or electromagnetic, as well as combinations thereof). During accidents at such facilities, environmental pollution can reach catastrophic proportions, threatening large regions and sometimes taking on a global character of environmental and energy danger. A lot is being done around the

world to prevent such disasters: effective means of passive and active protection of industrial facilities are being created, safe technologies and self-stabilizing operating modes (i.e., fundamentally stable modes) are being developed, etc. (Fig. 6.1).

Unfortunately, however, all technical means, systems, and complexes have finite reliability and limited-service life, and human (operator) actions and external factors can sometimes provoke (accelerate) the development of hidden structural defects or simply create a conflict situation where an accident becomes inevitable. Under such conditions, it is very difficult to predict or detect in a timely manner (i.e., at an early stage) dangerous developments that will undoubtedly lead to a serious accident and take measures, if not to prevent it (which is not always possible due to a lack of adequate control measures and a shortage of time), then at least to minimize its consequences. Along with man-made pollution of the environment, there are also processes of natural pollution caused by large-scale forest fires, volcanic eruptions, earthquakes, floods, etc.

Communal energy is the sector of housing and communal services that requires the largest amount of fuel resources. The need for daily hot water supply throughout the year and the need to provide heat during the cold periods of the year require the consumption of large amounts of fuel. This problem has two aspects – economic and environmental – which are closely intertwined. Energy and resource conservation is an urgent problem for humanity, which is closely linked to the environmental problem. Therefore, for example, solving the problem of fuel conservation (which is the one aspect of energy conservation) clearly contributes not only to the normalization of the country's economic life, but also to the improvement of the environment, and creates the foundation for raising living standards.

The problem of energy conservation can and should be solved in several ways, the main ones are the following:

- ***regulatory and organizational***, which involves creating conditions for stimulating energy-saving measures by developing appropriate legislation, standards, management and control structures, incentive funds, etc.;
- ***technological***, which involves the most rational use of existing technologies by optimizing them through the widespread use of computer technology or the use of fundamentally new technologies;

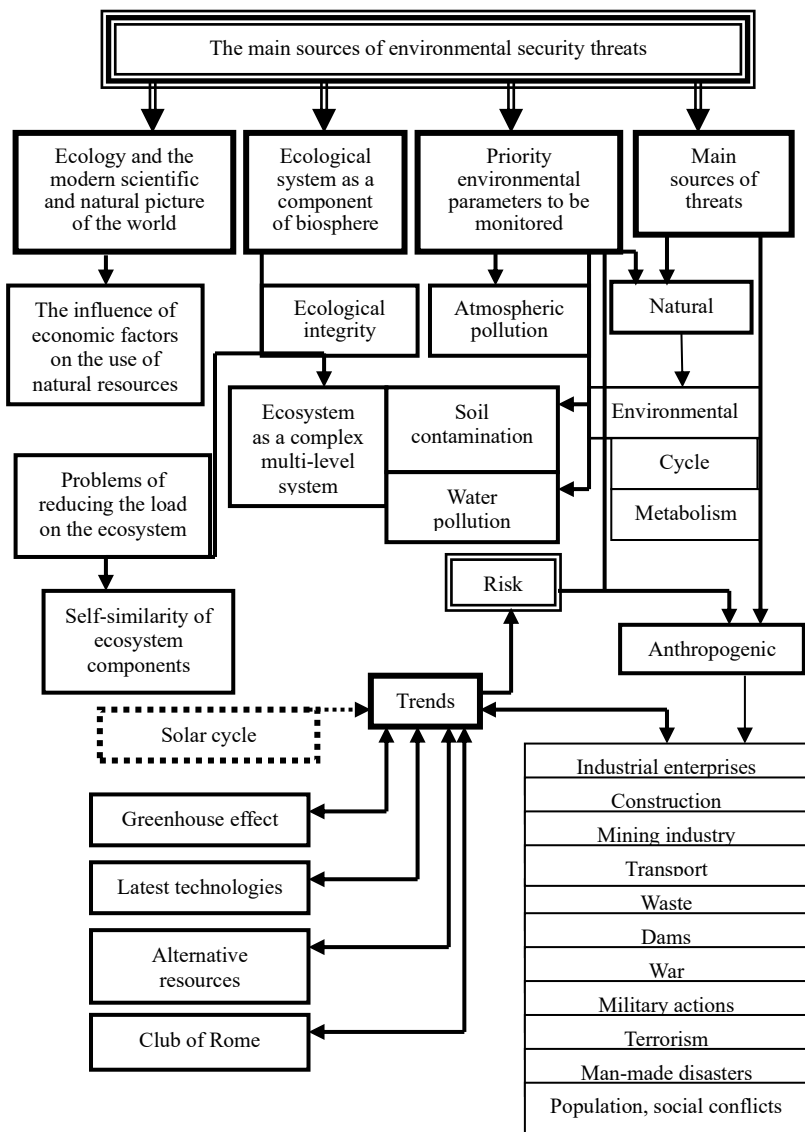


Fig. 6.1. Strategic aspects of energy and environmental safety

- **research and development**, which involves the development and implementation of new designs for power-generating units, components, and assemblies for the storage, conversion, and transportation of energy, as well as for its efficient use;
- **systemic**, which involves the development of the most efficient (from all points of view) systems for transporting energy from producers to consumers and its further distribution among consumers;
- **monitoring**, which involves the development of methods and measures for the continuous monitoring of the quantity and quality of both the energy produced and that used by consumers, as well as the state of the environment in the area affected by power-generating units;
- **utilization**, which involves developing measures to use the portion of energy that is normally lost (dissipated) or to use solid waste, biomass, and waste products as fuel.
- **alternative**, which involves using alternative (renewable) energy sources instead of (or in addition to) traditional ones.

Optimization of existing technologies is no less important from the point of view of ensuring environmental and energy stability. In technologies with extreme operating characteristics (i.e., characteristics that have a clearly defined maximum efficiency function) and factors that influence the achievement of these extremes, which tend to change unpredictably, it is advisable to use optimal control in order to keep the process at the maximum efficiency function at all times. This ensures significant resource savings, regardless of the influence of various factors.

It is also advisable to save natural resources when using existing technologies, i.e., not extracting (not using) resources more than it is necessary to meet current needs. For example, installing automatic light switches in stairwells that turn off the light for a period of time sufficient for an elderly person to reach the next floor, which (like all other floors) is also equipped with such switches, can provide daily savings of up to 20 kWh per hour per stairwell of a 16-story building, or more than 7,000 kWh per year, which corresponds to savings of about 850 tons of coal [2]. This is equivalent to 7,000 kWh per year, which corresponds to a saving of about 850 tons of coal [2]. Another example is limiting outdoor advertising to the hours when there is evening (night) passenger traffic, turning off part of street lighting at night, etc. Another example of savings is the use of transport units with greater cargo or passenger capacity to provide transportation, as this significantly reduces specific energy consumption. Significant fuel savings

can be achieved by using transport solutions that eliminate the problem of stopping at traffic lights and thus ensure more economical engine operation.

Thanks to the resource savings, between 1980 and 1990 years, the average energy intensity of production worldwide decreased by 20%, and in developed countries by 30%. Since 1984, the US has been increasing its production of goods and services without increasing energy consumption, while Germany, the UK, and Japan have been reducing their energy consumption. In Japan, oil consumption per unit of output (compared to the late 1970s) has decreased by more than 2 times, and in the US, by more than 1.5 times. In the US, the mileage of a car using the same amount of fuel has increased by 1.5 times [3]. This has contributed to the fact that organic fuel production has reached saturation point, with a further decline predicted in the 21st century.

However, the most effective way to save resources is to use fundamentally new technologies that allow either to significantly save these resources (as in the case of using MHD generators instead of “classical” thermal power plants), or to use fundamentally different resources and to reduce significantly the absolute consumption of these resources, as is the case in nuclear energy. Indeed, the energy intensity of uranium ore is 30 times higher than that of coal, which means that less ore needs to be extracted and transported to meet the same energy consumption requirements. Incidentally, more uranium is extracted from coal than from uranium ore, and the content of radioactive substances (uranium, thorium, and some others) in emissions from coal-fired power plants is several orders of magnitude higher than in emissions from nuclear power plants (under normal operating conditions). The risk of death caused by a nuclear power plant is 1 person per 1 GW of capacity, while the risk of death caused by a coal-fired power plant is close to 100 people per 1 GW of capacity [2].

Waste disposal plays a significant role in solving the problem of resource conservation. Moreover, a significant portion of waste is actually raw material for other industries or a potential source of energy (fuel). For example, waste from the metallurgical industry (slag) is a valuable raw material for the production of artificial fibers, waste from the woodworking industry can be used as fuel, etc. Solid household waste can be a source of both secondary raw materials and fuel. Therefore, it is necessary to transform from measures and means of waste collection, accumulation, transportation, and disposal to the development of technologies for the complete use of waste as a source of raw materials and energy.

Another way to reduce resource consumption is to use alternative resources and energy sources. Today, there are various types of gas generators that allow combustible gas to be obtained for use in internal combustion engines and for heating boilers. Thus, metal-plastic structures are successful substitutes for wood, and composite materials replace rapidly the “traditional” metal structures, primarily in cosmonautics and aviation. Moreover, composites have much better design, operational, and special characteristics and properties, and their production has a significantly lower harmful impact on the environment and requires fewer resources.

Let develop a scale of indicators for each of the above ways to reduce energy costs (costs of implementation, time of implementation, risks, payback period, environmental impact, and versatility of the method), as it is shown in Table 6.1. Then assign corresponding linguistic relative values to these indicators, for example, Very high DV (1), High VL (0.75), Moderate PM (0.5), Low NV (0.25), None B (0), and assign negative or positive signs reflecting the corresponding impact on the final result to them. Then it is possible to compile a “spectral” characteristic of the specified paths, where the amplitude of each line of the spectrum represents the algebraic sum of the corresponding indicators and determines the priorities for using each of the paths.

Even from an approximate (qualitative) assessment, it is clear that the priority task for all enterprises that generate and consume energy is the economical (EK) generation, transportation, and consumption of energy, for which it is necessary to:

- use the latest technologies;
- organize continuous monitoring of energy consumption, energy conservation, and energy management;
- create effective mechanisms to encourage economical energy consumption and energy conservation;
- organize continuous improvement of staff knowledge and skills in the field of energy-saving technologies.

E/B coefficients can be presented in a simpler form as the ratio of the sum of the absolute values of payback (OK), universality (YH), and risk supplement (1-P3) to the sum of funds (KO) and implementation time (TP), i.e.

$$E / B = \frac{OK + (1 - P3) + YH}{KO + TP} .$$

Table 6.1

"Spectral" characteristic of ways to reduce costs

Ways to reduce costs for gas imports	Implementation costs	Implementation time	Risks	Pay-back	Environmental impact	Universality	Overall assessment
Price reduction (CI)	DV (-1,0)	DV (-1,0)	DV (-1,0)	NO (0,0)	NV (-1,0)	DV (1,0)	-3,0
Economy (EC)	VL (-0,75)	VL (-0,75)	NV (-0,25)	DV (1,0)	DV (1,0)	DV (1,0)	1,25
Waste disposal (UT)	DV (-1,0)	VL (-0,75)	PM (-0,50)	DV (1,0)	DV (1,0)	DV (1,0)	0,75
Alternative energy sources (AL)	PM (-0,5)	PM (-0,5)	NV (-0,25)	DV (1,0)	NO (0,0)	PM (0,5)	0,25
Alternative fuels (NT)	NV (-0,25)	NV (-0,25)	NV (-0,25)	DV (1,0)	NO (0,0)	PM (0,5)	0,75
Search for own deposits (PR)	DV (-1,0)	DV (-1,0)	VL (-0,75)	PM (0,5)	NV (-1,0)	DV (1,0)	-2,25
Search for own deposits (PR)	DV (-1,0)	DV (-1,0)	PM (-0,5)	VL (0,75)	DV (-1,0)	PM (0,5)	-2,25

The above, however, does not exclude the use of other, alternative methods of reducing the need for imported and domestic ‘non-renewable’ energy sources. Innovative research should be carried out in all areas, but taking into account available resources, opportunities, priorities, and external factors.

Any structures, enterprises, or residential buildings must be located in such a way that their activities do not affect adversely the environmental situation in the development area. This means not only minimizing possible pollution from emissions and discharges, but also minimizing acoustic, electromagnetic, thermal, and other types of pollution of the natural environment that may affect the living standards of residents or the state of the environment.

In addition, an important factor in maintaining ecological balance is the rational location of economic activities, primarily power generation facilities. For example, it is rational to build powerful power plants outside cities, taking into account wind patterns (so that for most of the year, the winds blow

from the city to the plant, thus carrying the emissions from its chimneys away from the city). However, when it comes to housing and communal services facilities such as heating boiler rooms, it is rational to build them in the center of the area they serve in order to minimize heat loss, and thus reduce resource consumption. In other words, heat sources should be as close as possible to heat consumers. At the same time, solid waste processing plants, which should completely replace existing landfills, should be built not only in accordance with the requirements for power plants, but also taking into account the geological structures in the area of the plant.

Some of the above measures are already being implemented in the housing and utilities sector, primarily in heat supply systems, which are among the largest consumers of energy resources in the urban economy. Unfortunately, these costs are not justified: up to 20–30% of heat (and, accordingly, the energy resources used to produce it) is lost by heating networks due to poor insulation, and almost as much is lost due to the destruction of heating networks by corrosion. These are very significant costs, and the big part of energy conservation efforts is aimed precisely at eliminating the causes of these costs. A lot of positive changes have already been made, primarily through the use of the latest technologies in the creation and laying of new types of heat transport networks, the development of more efficient centralized heat supply schemes and systems, and the use of more successful designs for heat-generating units (integrated production of electricity and heat using combined steam-gas and gas turbine units), and bringing heat supply sources as close as possible to heat consumers. These measures make it possible to reduce the above-mentioned unproductive costs by 2.5–2.7 times. But there is another way to save energy: increasing the efficiency of the heat-generating units themselves, i.e., optimizing the fuel combustion process and utilizing the energy from combustion products.

Today, in order to ensure complete combustion of gas in the boiler furnace or gas turbine, sufficient air is supplied to the furnace (to the turbine combustion chamber) with a sufficiency coefficient of about 1.15. However, this approach is not optimal because it does not take into account the actual composition of air and gas and, moreover, does not take into account the dynamics of the process, when a change in load may require an additional oxidizer (or, conversely, a reduction in air supply). This can result in either incomplete fuel combustion and the associated fuel overconsumption and additional pollution of the atmosphere with incomplete combustion products, or cooling of the furnace (turbine combustion chamber) with air that does not

participate in the combustion process and only worsens the thermal (and economic) characteristics of the thermal unit, since an additional amount of fuel will have to be consumed to produce the specified amount of thermal energy. In both cases, there is an unproductive consumption of energy resources. The problem that arises in this case can only be solved by applying automatic optimal control, when a self-adjusting device (based on a microprocessor) continuously analyzes the actual combustion process and, accordingly, maintains the optimal mode by ensuring the appropriate air/fuel ratio that corresponds to both the actual characteristics of fuel and air and the current requirements of the thermal unit. The criteria for optimizing the combustion process can be the minimization of carbon monoxide (CO) with simultaneous minimization of air consumption (this path is quite difficult, as it requires the use of an expensive and, moreover, insufficiently reliable gas analyzer in real operating conditions, together with an extreme regulator), or the achievement of the maximum temperature in the furnace (combustion chamber) at a constant (fixed) fuel consumption by varying the amount of air supplied to the furnace (combustion chamber), i.e., extreme air supply control. The latter approach has already found application in control systems for gas turbine engines in aircraft and ships, as well as in large stationary power units.

A promising source of resource conservation is the use of organic waste as fuel. This requires the preliminary sorting of waste accumulated as a result of the activities of residents of residential buildings, its briquetting (or other method of concentration), as well as the use of special gas generators that produce combustible gas from organic fuel, which then is fed into the furnace of a heating boiler. This method of using alternative fuel can provide significant savings in heating costs.

A combination of measures such as reducing heat energy consumption through low thermal insulation and corrosion using the latest technologies, improving centralized heat supply schemes, bringing consumers closer to heat-generating capacities, using modern computer control systems along with the utilization of combustion products and taking into account the actual ambient temperature (for appropriate regulation of the water temperature at the entrance to the heating network), as well as the utilization of organic household waste, ensure sustainable and significant energy savings in heating systems and increase energy safety.

One of the promising areas of energy conservation in the housing and utilities sector is water treatment, water supply, and wastewater disposal,

which require a significant amount of electricity and other resources (primarily chemical reagents) for their implementation, which are not always used efficiently. This is due, on the one hand, to insufficient ‘transparency’ of the physical and chemical processes of water purification and disinfection, and on the other hand, by the imperfection of technical means and procedures for monitoring the state of water in reservoirs, at the inlet and outlet of treatment facilities. In addition, resource overconsumption is closely linked to the imperfection of the design and condition of water distribution networks and accounts the big volumes of all water losses (and thus electricity losses). Finally, wasteful consumption of resources is partly due to the lack of adequate reliable models for the functioning and operational changes in the condition of individual components of water treatment, water supply, and wastewater disposal systems, which complicates the problems of operational technical diagnostics and maintenance of equipment based on its actual condition and does not allow for the timely repair (or replace) this equipment in a timely manner, preventing its failure during operation.

Energy and resource conservation in the disposal and processing of solid and liquid waste also has certain perspectives. Firstly, solid and liquid waste can become a source of secondary raw materials, the production of which is much cheaper (such as the extraction of ferrous metals from waste using magnetic devices or the extraction of non-ferrous metals using chemical or physical methods) than the production of primary raw materials, or even if it is more expensive, it does not require the use of natural resources that may be inaccessible (for example, located outside national borders) or depleted. Secondly, solid waste can be used as a source of raw materials for the production of glass, paper, etc. Finally, solid organic waste can be used as fuel, creating conditions for saving natural fuel resources. A prerequisite for the use of solid waste as a source of natural resources and fuel is its prior sorting at processing (sorting) sites. Radioactive waste is a separate issue. Modern science and technology are largely unable to utilize this extremely toxic hazardous waste from the nuclear fuel cycle. Therefore, the issue is their reliable long-term disposal in places where they can be stored safely (for example, in karst caves, which are carefully guarded and monitored for possible migration of radionuclides into the soil) in special sturdy, corrosion-resistant, watertight containers for hundreds of years – until technologies for their disposal are invented. Therefore, waste disposal is a reliable way to conserve resources.

The above measures can significantly reduce the consumption of natural resources and contribute to maintaining the balance in the ecosystem and the development of innovative resource-saving and environmentally friendly technologies.

Three stages can be identified in the development of such technologies:

- search for the most efficient technologies in terms of productivity;
- search for the most efficient technologies in terms of product quality;
- search for the most efficient technologies in terms of resource conservation.

The first two stages have already passed their ‘peak’ of development, and although they continue, they are already on the verge of saturation, i.e., efforts aimed at finding new technologies lead to insignificant shifts in these areas (of course, within the limits of existing “traditional” scientific concepts and on the basis of modern technology). Here, significant breakthroughs are possible only under the condition of revolutionary leaps caused by discoveries in such areas of science as crystal physics, bionics, thin film physics, physical chemistry, nuclear physics, etc. Unlike the first two stages, the search for resource conservation has only just begun, and the first results give reason to believe that significant results can be achieved in this area.

The use of computer control systems has a noticeable effect on resource conservation:

- in transport, it ensures optimal engine operation, taking into account the terrain, changes in direction, acceleration or braking, load, etc.;
- in municipal energy, it facilitates predictive heat supply management, which improves service quality and at the same time contributes to fuel savings;
- in traffic control, it optimizes the frequency of traffic light changes and the duration of traffic on each of the controlled sections of the road, taking into account the actual and expected traffic densities on the highways, which contributes to both fuel savings and environmental improvement, as well as increasing the average speed of traffic;
- computer control of complex processes allows timely (or even proactive) changes to modes, taking into account mathematical models of processes and actual values of various factors or their derivatives, ensuring minimization of resource and energy costs;
- in dynamic transport planning, the use of appropriate computer programs allows the selection of optimal routes, optimal means of transport,

and optimal traffic flows in order to save fuel, make efficient use of rolling stock, and achieve the full volume of transport within the specified (or shortest) time frame.

There are many other examples of the use of new technologies to ensure resource and energy conservation, including in the housing and utilities sector, but most of them rely on new technologies for waste and energy recovery. Today, when resource and energy consumption reaches enormous proportions, it is necessary to recognize that the current rate of resource use threatens to exhaust their known sources within the next half-century to century. There is an urgent need to recycle industrial and other human waste, as well as energy, in order to slow down the rate of depletion of natural resources and replace them with “secondary” raw materials and ‘secondary’ energy obtained through recycling.

One of the first attempts at energy recovery is the use of hot gases emitted from boiler furnaces or metallurgical furnaces to heat water or air for further use in industrial or domestic applications. This approach saves a significant amount of fuel and helps to reduce the environmental impact.

Another example of energy recovery is the use of biogas (mainly methane), which is released during the wastewater treatment process in the biotanks of treatment plants and is a product of the vital activity of bacteria that assimilate organic substances of wastewater. Biogas is used in heating boilers to heat water for domestic and technical needs, which reduces overall fuel requirements and thus contributes to resource conservation [4–5].

Today, the environmental situation in Ukraine is significantly deteriorating due to the existence of solid waste landfills. This is evidenced by the fact that Ukraine ranks among the lowest in Europe in terms of the environmental condition of solid waste landfills. In cities, more than 1.1 kg of solid waste is generated per capita per day. 35 million cubic meters of solid waste that are collected and transported to landfills (“dumps”) annually, have the organic fraction from 17% to 82%, i.e. from 1.5 million tons to 7.18 million tons. About 85% of the components of solid waste (i.e. 1.3–4.8 million tons) are subject to oxidation. Today, this oxidation occurs either “naturally” or through the incineration of solid waste. In both cases, between 1.6 million tons and 5.9 million tons of carbon dioxide are emitted, and the energy contained in the organic components of solid waste is either lost irretrievably or used extremely inefficiently [1]. To prevent that, it is necessary to implement widely gas generator technologies that solve two problems simultaneously: clean up large areas from solid waste and utilize

the latter to obtain energy. During the gasification process, fuel and oxygen from the air, which is fed in limited quantities into the gas formation chamber, are heated by the incandescent reactor (due to the combustion of a small portion of the fuel) and react with each other, resulting in the decomposition of solid waste into carbon, water vapor, resins, and oils, and the subsequent reaction between oxygen and carbon provides a temperature sufficient for the formation of combustible gas – carbon monoxide CO. Resins and oils decompose into gases containing hydrogen and, partially, methane, which are also combustible gases. Compared to simple incineration of solid waste, gasification has a higher energy efficiency (gas consumption per unit of thermal energy produced in gas generators is by 1.5–2 times lower than during direct incineration of solid waste in boiler furnaces).

Other examples of solid waste utilization include the use of metallurgical industry waste (slag) as raw material for the production of artificial fibers, or the use of solid residues from the biological treatment of wastewater as natural fertilizers. Utilization involves not only the use of waste from one or another production process (including energy released during the production process and, in the absence of measures and means for its utilization, simply dissipated into space) in other technological processes, but also the use of waste in a repeat production cycle. For example, waste paper can be reused to produce paper, which saves wood (and thus contributes to environmental protection). Broken glass can be reused to produce glass products, which saves ingredients that would otherwise have to be extracted from quarries. The use of scrap metal reduces ore mining and energy consumption, etc.

There is also an actual problem of using alternative technologies to optimize environmental protection activities. As a rule, different (alternative) paths can be taken to achieve a particular goal. At certain stages of technological development, the main criterion for the acceptability of a technology was, as a rule, the “efficiency/cost” criterion. However, in the context of the looming environmental crisis and the depletion of currently explored natural resources, the criteria of environmental friendliness of technologies and minimal consumption of natural resources are coming to the fore. Here, it is necessary to reconsider alternative ways of achieving the set goal in terms of using the most environmentally friendly and resource-efficient technologies.

6.2. Scientific basis for risk-oriented management of energy and environmental safety

Sustainable energy and environmental safety is the basis for preventing and solving environmental problems, which guarantees sustainable development for the country's citizens. The development and improvement of methodologies for increasing environmental safety and the introduction of innovative energy-saving and environmentally friendly technologies are extremely pressing issue, allowing the study of factors that increase the efficiency of resource use and ensure energy and environmental safety.

The main factors characterizing the risk of an energy or environmental disaster include the following:

V_S – increased probability of disaster (due to external and internal factors), which takes into account external factors (natural: tectonic activity, electromagnetic activity, meteorological activity; socio-political, military, and economic crises, etc.) and internal factors (wear and tear of technical equipment – “aging,” low staff qualifications, emotional stress, etc.);

V_W – reduction of the probability of a disaster through regular staff training, regular checks of the physical and psychological condition of staff, ensuring optimal operating conditions, etc.;

V_O – situations that could trigger a disaster (technogenic or natural disaster in a region close to the region under consideration or associated with possible common consequences);

V_T – situations that could ‘freeze’ (slow down) the development of a disaster.

The risk assessment process technology can be implemented as shown in Fig. 6.2.

With regard to the quantitative assessment of the possibility of a disaster E_{Op} , it is necessary to take into account all categories of SWOT analysis factors [2], and the following empirical expression can be proposed to assess the possibility of a disaster:

$$E_{Op} = p \cdot F \left\{ \max \left(\mu \left[V_{Si}, V_{Oj} \right] \right) - \min \left(\mu \left[V_{Wm}, V_{Tn} \right] \right) \right\},$$

where V_y – factor of the y -th category ($y \in [S, W, O, T]$), $\max$ and $\min$ – multi-valued logic operators, F and μ – corresponding functionals, p – correction coefficient that takes into account the degree of risk increase under conditions that differ from the average.

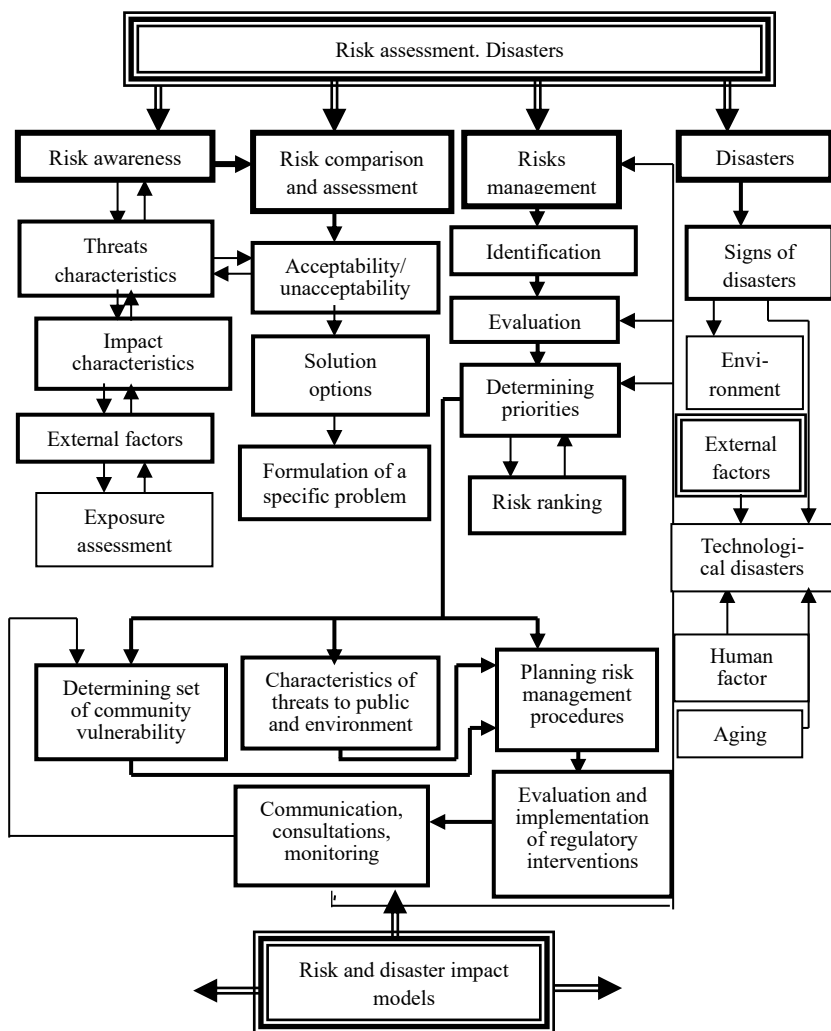


Fig. 6.2. Intellect-card of the risk assessment process

The coefficient p can be determined from the following empirical expression:

$$P = \left\{ \frac{\beta + 1}{N - \beta + 1} \right\} \{ [1 + \sum_1^N (x_i)] \},$$

where N – total number of indicators that can characterize external and internal influences on the risk value, β – number of indicators actually taken into account, $x_i = 1$, if it is taken into account, and $x_i = 0$, if it is not taken into account.

If information about the technical condition of a complex technical system is available, i.e., the level of individual reliability Y_i (H – High, M – Medium, L – Low), fuzzy input disturbance variables X_j and the causes of the influence of fuzzy input variables are known, then M_Σ – the output linguistic variable, which evaluates the technical condition of the system in terms of H, M, L, can be represented as follows:

IF $(Y1) \subset (L, M, H)$ ***AND*** $(Y2) \subset (L, M, H), (Y3) \subset (L, M, H),$ ***THEN*** $M_\Sigma \subset (L, M, H)$

The management of complex technical systems of the treatment technologies takes place under conditions of limited (incomplete) and unclear information, which affects the efficiency of processes. This is due to the fact that the environmental indicators of the systems are not usually determined online and, in addition, certain averaged data are used. At the same time, regulatory measures aimed at achieving effective management may become inadequate for the current situation, and there is a risk of losing control over the treatment or disposal processes.

Every situation in the management of environmental protection facilities in a complex situation with unclear and incomplete information or decision-making is characterized by the presence of risks that should be taken into account.

The following types of risks are possible:

- development risks (incorrect choice of an inadequate design direction, unsuccessful architecture or structure, lack of prospects for further use of the development);
- production risks (manufacturing, assembly);
- risks of operation and maintenance (information provision, operating environment, safety);

The risks listed above can be classified as the following:

- risk of underestimating the impact of a factor;
- risk of overestimating the impact of a factor;
- risk of error in determining the magnitude of a specific factor;

- risk of general misjudgment of the situation;
- risk of error in determining the possible consequences (current and future) caused by all the previous risks.

In this case risk-oriented management involves:

- identifying key indicators that need to be achieved;
- establishing parameters or factors that affect results;
- identifying factors that are key to the occurrence of risk;
- reducing the probability and cost of each risk;
- developing measures to mitigate each key risk;
- developing management plans that track changes in the situation.

There are two types of risk-oriented management:

- considering the problem from the perspective of possible threats (identifying each threat, its probability, and cost);
- considering the problem from the perspective of the effectiveness of achieving the aim (what key results should be achieved, what factors or parameters can affect the result, what key factors influence the achievement of the goal, what is the probability and cost of each risk).

To assess risk, it is necessary to have an understanding of the threats that are characteristic of certain factors in the context of specific parameters of the operating environment, as well as to feel the connection between understanding the processes that determine the sensitivity of factors, the relevant dynamics of processes, and the degree of adequacy, reliability, and unambiguity of this response (Fig. 6.3).

This relationship can be represented as a sequential transition from a single factor and a single parameter with a single relationship to a complex system under the influence of a number of factors, parameters, and relationships that can be combined using certain extrapolation procedures.

The risk awareness procedure is performed by following these steps:

- identification of risk;
- identification of possible consequences in case of risk realization;
- assessment of the probability of various possible consequences;
- assessment of the probability of risk minimization;
- assessment of the maximum consequences in case of risk realization.

Risk identification includes the following types of approaches:

- aim-oriented (any event that threatens the achievement of the goal is identified as a risk);

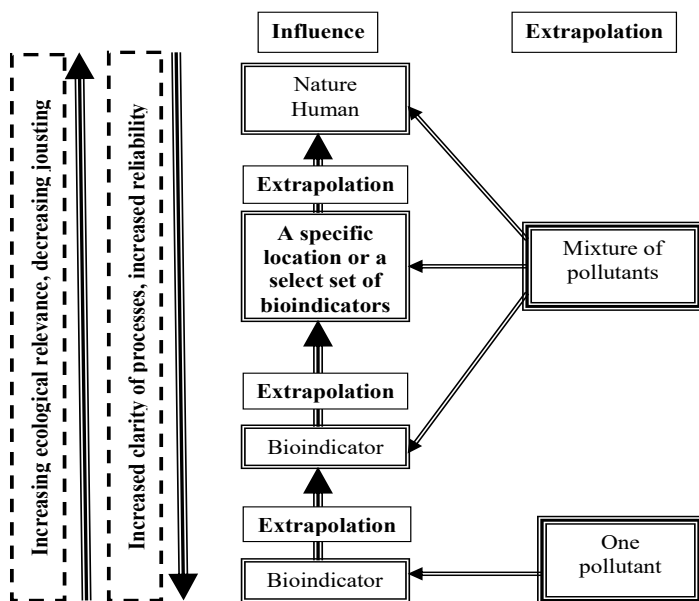


Fig. 6.3. The relationship between understanding processes, reliability and relevance

- action plan based (various scenarios for achieving the aim are considered, and any event that could lead to the development of an undesirable scenario is considered a risk);
- systematic (a questionnaire is compiled based on a systematic approach and knowledge of positive experience, and analysis of the questions may reveal risks);
- overall risk checks (sometimes there are lists of possible risks that are compared to a specific situation);
- risk ranking (all resources are classified by risk, or all threats are considered in terms of their impact on resources, or the consequences are considered and analyzed to determine which combinations of threats and resources lead to them).

Once the risk is identified and assessed, the following approaches to risk management are used:

- avoidance (exclusion);
- reduction (mitigation);
- containment;
- transfer (insurance).

The risk indicator (risk price) VaR indicates the maximum losses that should not be exceeded for a given probability and confidence interval in a given time interval. Usually, a time interval of 1 year can be used in housing and communal services systems. The confidence level (i.e., the probability that VaR will not exceed the maximum acceptable loss) is usually $\alpha = 0.95$ (i.e., 95%). The VaR value can be represented both in monetary terms of losses and in any other values. Then, at a given level $\alpha \in [0,1]$, VaR is set as the smallest number q at which the probability P of losses Q exceeds q by an amount that is not greater than $(1 - \alpha)$:

$$VaR_{\alpha} = \inf\{q \in \mathfrak{R} : P(Q > q) \leq 1 - \alpha\}$$

Here, $\inf$ determines the upper bound, $\mathfrak{R}$ – set of possible losses. In probabilistic terms, VaR is defined as the quantile of the loss distribution.

There are other approaches for assessing the acceptability of certain types of equipment for normal operation and predicting possible failures, which are based on test data and the determination of parameters of accelerated thermal or mechanical aging, or “aging” of information, but they are acceptable only in cases where reliable statistics exist and risks caused by external factors are not considered [2, 6–7].

References

1. Єремєєв, І. С., Дичко, А. О. (2024). Техногенні та екологічні ризики і катастрофи: підручник. Одеса: «Олді+». 234 с.
2. Єремєєв, І. С., Дичко, А. О. (2022). Екологічна природна та техногенна безпека: підручник. Одеса: Видавничий дім «Гельветика». 434 с.
3. Зеркалов, Д. В. (2007). Екологічна безпека: управління, моніторинг, контроль: навчальний посібник. К.: КНТ, Дакор, Основа. 412 с.
4. Stepanenko, A. V. (2014). Environmental and economic strategies in system of environmental safety endurance. Наука та наукознавство, №

4, pp.77–89. Available at: http://www.irbis-nbuv.gov.ua>irbis_nbuv>cgiirbis_64

5. Yermeyev, I. S., Dychko, A. O., et. al. (2023). Measuring, forecasting and monitoring sustainability of biochemical wastewater treatment in war period. Vcheni zapysky Tavriys'koho natsional'noho universytetu imeni V. I. Vernads'koho", seriya "Tekhnichni nauky", 34 (73), № 4, pp.183–191. Available at: https://www.tech.vernadskyjournals.in.ua/journals/2023/4_2023/29.pdf

6. Dychko, A. O., Remez, N. S., et. al. (2024). Forecasting the risks of man-made and ecological disasters. IOP Conference Series: Earth and Environmental Science. IOP Publishing, 1348, 1, p. 012011. <https://doi.org/10.1088/1755-1315/1348/1/012011>

7. Dychko, A. O., Yermeyev, I. S., Remez, N. S., Minaieva, Yu. Yu. (2025). Analysis of risks to the environmental safety of water treatment. Vcheni zapysky Tavriys'koho natsional'noho universytetu imeni V. I. Vernads'koho", seriya "Tekhnichni nauky", 36 (75), № 2, pp. 241–246. <https://doi.org/10.32782/2663-5941/2025.2.2/33>

Section 2

Dialectics of Global, Regional and National Security

Chapter 7

Global issues of the modern world and European security

(R. Kliuchnyk, E. Lymonova)

By the end of the first quarter of the 21st century, the world has faced large-scale challenges that go beyond both national and regional borders. Globalization, while promoting transparency and mobility, also generates new environmental, social, economic, and political threats. Europe, as a center of integration processes and one of the leaders of global development, is confronted with the consequences of these global transformations. Climate change, energy crises, uncontrolled migration, terrorist threats, poverty and unemployment, and value-based conflicts – all of these factors affect stability and security in Europe. Therefore, the study of global, regional, and national security is of particular importance. By analyzing the nature of contemporary global challenges and their impact on the European space, it is possible to forecast the capacity of a united Europe to respond to the challenges of the present and the future. It is also worth noting the fragility of the very idea of European integration: Eurosceptic movements indicate the uncertainty of part of the European population regarding the future of the European Union. This set of issues is especially important for Ukraine in the context of its European integration. The aspiration to become a member of the EU must also be supported by readiness to participate in its security policy.

7.1. Globalization, global problems, and security threats

The concept of globalization occupies an important place in contemporary political and economic discourse. It manifests itself in the growth of international exchange and the increasing interdependence of states, the spread of universal standards of production and consumption of goods and services, and the strengthening of international ties. The

integration of markets for goods, services, and labor, as well as the formation of a unified information space, are integral features of the development of the modern world. Europe has always occupied an important position in globalization processes; therefore, this issue is particularly relevant within the framework of research on European security.

It may be appropriate to speak of globalization processes as early as the late fifteenth century. This period marked the beginning of the Age of Discovery, which shaped Europeans' perceptions of the world, including its regions distant from Europe, above all the Americas. The formation of colonial empires constituted an important component of the globalization process. Great Britain, France, Spain, Germany, the Netherlands, and other European countries seized territories across the globe, not only expanding the presence of European civilization but also shaping the contours of international trade and the global market.

Both world wars became a logical consequence of globalization. States united into powerful coalitions with the aim of reformatting the system of international relations and achieving global dominance. Globalization processes continued during the Cold War, which became a period of struggle between the capitalist and communist systems for influence over the countries of the so-called Third World. The contemporary world likewise represents a space that is constantly undergoing globalization.

Globalization can be considered in various dimensions: economic, social, political, cultural, technological, and others. At the same time, attitudes toward this process largely depend on the ideological and worldview orientations of the author or speaker.

The economic dimension of globalization consists, in particular, in the integration of national economies into the global system through international trade, investment, migration, digitalization, and so on. The significant impact of globalization on national economies is evident, and it includes both positive and negative components. The positive impact occurs through the acceleration of technological development via the exchange of knowledge, increased competition, access to new markets, and investment. At the same time, there is a "high risk of growing dependence on foreign technologies, possible deindustrialization of the country's economy, and loss of competitiveness of national producers" [1, p. 198]. One of the most visible manifestations of globalization was the global financial crisis of 2008. Precisely because of the close interconnection of the world's economies, a crisis that began with the bankruptcy of a single American bank spread

worldwide. O. Zhukova emphasizes the ‘other side of the coin’: governments and central banks ‘coordinated fiscal and monetary policies in order to counteract the decline in consumption, restore confidence in securities markets, and encourage lending’ [2, p. 464].

Economic globalization is not without reason regarded as a factor of economic growth, entrepreneurial freedom, prosperity, and inclusive development. By ‘inclusiveness’ is meant such growth that promotes shared prosperity and accelerates the reduction of poverty and inequality [3, p. 693]. S. Swadźba, examining globalization, arrives at certain conclusions, among which are the following statements:

1. The level of globalization in the world economy has increased significantly over the past 50 years. This applies both to globalization as a whole and to its economic dimension.

2. The increase in the level of globalization (not always uniform) has occurred across all groups of countries, distinguished both by income per capita (high-income, middle-income (upper-middle and lower-middle), and low-income countries) and by geographical criteria (Europe and Central Asia, Sub-Saharan Africa, North America, etc.).

3. The highest level of globalization is observed in high-income countries, and from a geographical perspective, in Europe and Central Asia as well as North America. The lowest level is found among low-income countries, and geographically in South Asia and Sub-Saharan Africa.

4. In recent decades, a slowdown in globalization (slowbalisation) has been observed, and following the COVID-19 pandemic, deglobalization has also taken place. However, such phenomena have been encountered in the past as well, albeit on a smaller scale.

5. In the long run, we are likely to face a slowdown in globalization (slowbalisation) with short phases of deglobalization. Globalization is not facilitated by an unstable socio-political situation in the world. Moreover, the potential for high rates of globalization growth has already been exhausted; such opportunities remain only for low-income countries, which have so far been least affected by globalization [4, pp. 19–20].

Transnational corporations play an important role in globalization processes. They are capable of stimulating the development of global innovation and learning by creating a favorable organizational environment and ensuring the effective functioning of their centers of competence. The outcomes of these processes of innovation and learning are then transmitted to international organizations. Countries around the world can benefit from

these innovations and learning experiences in order to improve product quality or significantly reduce operational costs. As a result, there is an opportunity to enhance the level of consumer satisfaction [5, p. 147]. At the same time, these companies create jobs and disseminate the business culture of their home country.

The phenomenon of lobbying is also associated with globalization and the expansion of transnational corporations (TNCs). It is widespread across different countries and regions and is characterized by varying degrees of regulation. In post-Soviet countries, lobbying often takes a concealed form and is aimed at protecting the self-interested goals of a limited circle of oligarchic groups, whose effectiveness in the lobbying process is determined both by their political influence and by non-public connections, as well as their capacity for informal decision-making [6, p. 113].

In our view, the social dimension of globalization consists in the erosion of boundaries between human communities worldwide. In recent decades, international mobility has increased rapidly, driven by the development of international transportation networks, the tourism industry, and the expansion of labor migration, among other factors. Digital transformation and the development of Internet-based communication have become important drivers of the spread of remote work and education. The expansion of high-speed Internet access, cloud services, messengers, video conferencing platforms, and collaborative work tools has created the preconditions for stable and efficient professional activity without physical presence at the workplace [7, p. 100]. This has led to the emergence of the phenomenon of digital nomads, which combines economic, technological, and social aspects of globalization. Naturally, this group includes not only IT specialists (although they are undoubtedly among the pioneers of remote work), but also teachers, psychologists, marketers, and representatives of creative professions. Digital nomads often have higher incomes than local residents and thus stimulate economic development.

At the same time, the new realities created by this way of life and work naturally give rise to concerns, as it erodes political borders and complicates the control and regulation of people; a kind of ‘escape’ from the state can be observed. These challenges established categories and practices of contemporary social citizenship [8, p. 303]. At the same time, some countries deliberately seek to attract digital nomads, such as Croatia, which is recognized as a desirable destination for this category of workers, in part due to a well-regulated legal and regulatory framework [9, p. 38]. Moreover, this

lifestyle facilitates social adaptation in a new environment and creates preconditions for intercultural dialogue.

Even without being digital nomads, almost anyone with Internet access can, with minimal effort, connect with people from other countries, learn about life in virtually any part of the world, build their own network of acquaintances, and maintain contact. These unprecedented opportunities expand people's social circles, which is particularly relevant for those who, for certain reasons, face difficulties in communicating with compatriots. The creation of virtual communities based on shared interests, rather than territorial or professional criteria, can also be seen as a manifestation of globalization in its social dimension.

Digital nomads can be regarded as a type of migrant (although there are different opinions on this), but global migration is not limited to them. People leave the countries where they were born on a large scale and attempt to move to places where they perceive life to be better. Not all migrants fully accept the "rules of the game" that exist in the countries where they settle, which can lead to conflicts.

The Internet technologies briefly discussed above are also a manifestation of technological globalization. Similar technological tools are developed and widely used across all countries of the world, made possible by a range of factors, including increased exchange of knowledge, goods, and services. Technological globalization also implies the integration of citizens worldwide through a single virtual environment [10, p. 3]. International technology transfer is also spreading, among the main types of which are trade in licenses and technical know-how. The volume of the latter is difficult to estimate, since 'knowledge transfer does not often occur in the form of formal agreements between parties; for example, in the process of providing engineering services, during the purchase or lease of high-tech equipment, a manufacturing enterprise may transmit some of its technological secrets and knowledge to the client without this being formalized through a contract termination' [11, p. 73]. In a broader sense, technological globalization can also be understood as the dissemination of uniform standards in the production of devices and software. At the same time, standards for the creation, storage, and reproduction of information are being unified, which facilitates international cooperation among individuals, businesses, and states.

Cultural globalization has become possible thanks to all the other dimensions of globalization. Thus, the spread of mass media, television in

particular, shapes the contours of those multidimensional globalization processes that include interaction and transformation, identity and difference, universalism and particularism, as well as the process of transforming the universal into the particular and the particular into the universal [12, p. 60]. Practically unlimited opportunities for cultural globalization are provided by the Internet: in real time, people can learn how individuals live all over the world, explore (or even adopt) their everyday practices, leisure activities, and ways of life.

Media, technology, and transnational corporations play a key role in cultural homogenization [13, pp. 12–13]. A clear illustration of these processes can be seen, for example, in the offices of companies and banks, supermarkets, universities, and other institutions which, in different countries around the world, exhibit very similar organizational structures and spatial arrangements. The dominance of the Anglo-Saxon world in cultural terms is manifested in the spread of American cinema, pop music, and festive traditions. In recent years, retail chains in Ukraine have been organizing ‘Black Friday’ in November, which has no connection to Slavic culture and is instead associated with the celebration of the American holiday Thanksgiving. The spread of the English language and the use of Anglicisms in Ukrainian, Polish, German, and other languages are also manifestations of cultural unification. This is a phenomenon that was already observable two centuries ago, when French aspired to the role of a global language.

The political aspects of globalization are associated with the creation of supranational structures that exercise (or seek to exercise) global governance. Thus, the leading organization of the contemporary world is the United Nations. This organization, established in the aftermath of the Second World War, ‘provided that radical reform is undertaken, will continue to remain an important institution not only of multilateral diplomacy but also of global governance’ [14, p. 63]. In certain cases, the UN Security Council may even authorize the use of force in order to maintain or restore international peace and security [15].

The International Monetary Fund is an important organization from the perspective of international economics and politics. By providing loans aimed at stabilizing national economies, ‘the IMF usually puts forward a fairly standard package of requirements, which includes the privatization of large enterprises, the liberalization of prices and foreign trade, a tight monetary policy to stabilize the currency, the termination of subsidies for loss-making enterprises, the minimization of the budget deficit through cuts

to social programs and tax increases, and currency devaluation' [16, p. 19]. However, a certain degree of skepticism is expressed regarding the adequacy of the IMF group's measures 'in the context of the intensification of global challenges such as inequality, climate change, the debt burden of the poorest countries, slowing economic growth, and the threat of global war and terrorism' [17].

There are also other organizations that bring together the vast majority of contemporary states, such as Interpol, the Universal Postal Union, the World Trade Organization, the Red Cross, and others.

The political aspects of globalization are also manifested in institutional unification. For example, in almost all countries of the Global South, the same basic political institutions that emerged in Europe and the United States several centuries ago have been reproduced: parliament, president, government, and political parties. At the same time, the substantive content of these institutions may differ depending on the country and the specific features of its economic, social, and political development. In Mexico, elections are competitive, but electoral campaigns are often accompanied by a high level of violence (ahead of the 2024 general elections, 37 candidates were killed) [18]. Cameroonian President P. Biya has led the country since 1982, and a scenario involving the transfer of power to his son appears quite plausible [19, pp. 83–84]. Other countries of the Global South also often merely imitate democratic institutions, while political practices remain far removed from the ideals of a democratic, social, and rule-of-law state.

Thus, globalization takes place in various spheres and across different regions of the planet; however, its unevenness allows us to speak of systemic problems, which will be examined in greater detail below. At this stage, we consider it appropriate to focus on the phenomenon of anti-globalism, which is often viewed as a natural response to the problems associated with globalization.

The complexity of studying this phenomenon is conditioned, among other things, by the fact that it does not constitute a monolithic movement or organization. The ideological features of anti-globalism consist primarily in its focus on rejecting globalization as a process of economic and political expansion by the most influential countries in the world and by transnational corporations [20, p. 37]. In the future, anti-globalism may become a coherent ideological and political concept; however, at present we see no prerequisites for this.

Globalization inevitably leads to the spread of global problems, which can be conventionally divided into natural-ecological and socio-economic and political categories. All of these, in one way or another, pose a threat to Europe and Ukraine. Therefore, their study is of key importance for the analysis of contemporary European security.

7.2. Natural and environmental threats to contemporary security: challenges for the European Union

In the 21st century, the concept of security has acquired a broader meaning: alongside traditional military or political security, environmental, food, energy, and social security have come to the fore. Among global challenges, particular attention is drawn to natural and environmental threats, which are increasingly manifested as a result of climate change, environmental pollution, and the degradation of natural resources.

Let us clarify the essence of the term and the main factors of natural and environmental threats. Natural and environmental threats are factors that arise in the natural environment (or as a result of human intervention in it) and negatively affect human life, the economy, health, and well-being. Such factors include climate change, natural disasters, pollution of water, air, and soil, loss of biodiversity, and the depletion of natural resources.

Today, Europe is increasingly facing the consequences of environmental instability:

- Southern Europe (Spain, Italy, Greece) suffers from droughts and wildfires;
- coastal regions (the Netherlands, Belgium) face the threat of rising sea levels;
- Central Europe (Poland, the Czech Republic, Germany) experiences high levels of air pollution due to industrialization and the use of coal;
- across all EU regions, there is a recorded decrease in the area of natural forests, loss of protected areas, and the disappearance of biological species.

Droughts and wildfires are becoming increasingly severe and frequent problems in Europe, a trend exacerbated by climate change. Historical data indicate a rise in both the frequency and intensity of these events, which have a significant impact on ecosystems, agriculture, and public health. Addressing these challenges requires a combination of climate change mitigation efforts and adaptation strategies to manage the consequences of extreme weather events.

Europe has a long history of droughts, with one of the most severe and widespread occurring in 1540. More recently, in 2022, a severe drought was observed, affecting rivers, agriculture, and ecosystems.

Wildfires have always been an integral part of the development of the European landscape, particularly in the Mediterranean region. However, climate change has led to the expansion of fire-prone areas and an increase in the length of fire seasons even in traditionally cooler regions. The growing frequency of heatwaves and droughts in recent years has significantly intensified wildfire risk.

Droughts and wildfires can lead to forest degradation, loss of biodiversity, and changes in ecosystem dynamics. In addition, reduced water availability and crop damage caused by droughts and fires result in substantial economic losses for farmers. Infrastructure is also affected: wildfires can damage infrastructure such as power lines and buildings, leading to further disruptions.

Extreme heat and smoke from wildfires can cause respiratory problems, heatstroke, and other health issues.

The impact of natural and environmental threats on contemporary security remains significant. Natural and environmental threats are closely interconnected with other dimensions of security. Their effects are felt at all levels, from the local to the global level (Table 7.1).

According to the Ecological Threat Report 2024 by the Institute for Economics & Peace, approximately 1.3 billion people in 50 countries face high or very high levels of ecological threats. 82% of them live in Africa. The population of these countries is expected to grow by a further 51% by 2050 [21]. Such threats (droughts, water scarcity, and food insecurity) are increasingly becoming factors of instability and even conflict [22; 23].

Biodiversity is also experiencing a critical decline: according to the European Central Bank (ECB), wildlife populations have decreased by 69% since 1970, and the rate of extinction is dozens of times higher than the average over the past 10 million years [24]. The Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES) estimates that the global economy loses up to USD 25 trillion annually due to nature degradation, water scarcity, and food and health crises; at the same time, integrated solutions could create up to 395 million jobs and generate USD 10 trillion in opportunities by 2030 [25; 26; 27].

Economic security has a direct impact on the economic performance of the European Union. According to the European Environment Agency

(EEA), economic losses from weather- and climate-related disasters in the EU amounted to approximately EUR 738 billion over the period 1980-2023, of which EUR 162 billion (22%) was incurred in 2021-2023 alone. Hydrological hazards (floods) account for 44% of total losses, storm-related events (wind, lightning) for 29%, while heatwaves, wildfires, and droughts make up the remaining 27% [28].

Table 7.1

The Interconnection between natural and environmental threats and other dimensions of security*

No	Dimension of security	Description
1	Economic security	Weather-related disasters cause damage to infrastructure and the agricultural sector. Disruptions in supply chains of raw materials and energy.
2	Energy security	Instability in energy supplies (especially gas and oil) forces the search for alternatives. The active transition to renewable energy sources requires new technologies and policies of energy diversification.
3	Social security	Deterioration of living conditions (water scarcity, rising temperatures, deterioration of public health). Forced migration (so-called environmental migration). Rising social tensions due to unequal access to resources.
4	Food security	Declining agricultural yields due to droughts, soil erosion, pests, and diseases. Dependence on imports of agricultural products.
5	Health and sanitary security	Water and air pollution becomes a cause of respiratory diseases, cancer, and allergies. The risk of the spread of tropical diseases in regions where they were previously uncommon is increasing.

**Source: compiled by the authors*

An analysis conducted by the Green Finance Institute in collaboration with academic partners (Oxford, Reading, UNEP WCMC, NIESR) showed that nature degradation could reduce a country’s GDP by up to 12% by the 2030s – more than during the 2008 financial crisis (approximately 5%) or the COVID-19 pandemic (approximately 11%) [29]. Although this assessment concerns the United Kingdom, experts from the ECB, the European Commission, and EU think tanks acknowledge that ecosystem degradation and biodiversity loss pose a serious risk to the EU’s economic resilience and financial stability [24].

Here are several additional examples of the impact of nature degradation on the economic performance of European countries.

Central European floods (2024): a series of floods resulted in losses of €4–5 billion in the Czech Republic and neighboring countries alone, of which

€1.9 billion was insured. Total recovery costs across the region reached up to USD 10 billion, including damage to infrastructure and agricultural supply chains [28; 30].

Floods in Spain (October 2024): these events had significant economic and social consequences and were highlighted in the ECB's economic review as an example of increasingly frequent weather-related risks that heighten the risk of financial instability in the EU [30].

Energy security. Climate change exacerbates instability in energy supply chains (gas and oil), forcing states to invest in renewable energy and diversification. In addition, nature degradation significantly affects hydropower generation, as droughts reduce river flows; consequently, European countries are increasingly shifting toward solar and wind power generation

Social security. Water scarcity, soil depletion, and rising temperatures all undermine public health, contributing to allergies, respiratory diseases, and an increased risk of cancer. Moreover, environmental degradation acts as a catalyst for forced migration from rural areas or regions affected by extreme weather events, as people seek resources and safer living conditions. As a result, social tensions are already increasing due to the inability to meet basic needs (water, land, and food), especially in densely populated or economically disadvantaged regions.

Food security can be considered in light of certain changes in the environment:

1. Soil erosion and land degradation. According to the Joint Research Centre (JRC) and the European Environment Agency (EEA), soil erosion in the European Union reaches up to 1 billion tonnes annually, and approximately 24% of land is affected by water erosion, particularly agricultural areas. About 32% of agricultural land in the EU is at risk of degradation due to tillage practices or erosion [31]. Such soil degradation significantly reduces fertility and the long-term productivity of agricultural production.

2. Droughts, heat stress, and agriculture. In 2025, losses caused by extreme weather events in the EU agricultural sector are estimated at €28.3 billion annually, which accounts for approximately 6% of agri-food production; half of these losses are caused by drought. Only 20–30% of losses are insured [32]. Moreover, the spring of 2025 in Northwestern Europe was the driest in a century: around one third of the territory was affected by orange and red warnings, which puts crop yields at risk, with losses potentially

reaching 20–30% on individual farms [33]. According to the European Environment Agency (EEA), the area where drought affected vegetation productivity in 2023 amounted to 143,500 km² (3.5% of the EU territory), including 66,500 km² of agricultural land, more than the twenty-year average (2000–2020) [34].

3. Climate change, pests, and diseases. Rising temperatures and changes in precipitation patterns lead to fluctuations in crop yields, an increase in pest populations, and the spread of plant diseases, which complicates agricultural productivity, particularly in the southern regions of the EU [35; 36].

4. Dependence on raw material imports. Although the EU is generally self-sufficient in most cereals and vegetables, it remains highly dependent on imported raw materials such as soybeans, maize, cocoa, and coffee. As of 2025, more than two thirds of imported fertilizers and agricultural products (including cocoa, soybeans, maize, and wheat) originate from countries with low preparedness for climate change and degraded biodiversity, which increases supply risks and price volatility [37]. The EEA also warns that more than 44% of future agricultural imports could become vulnerable to droughts by 2050 due to climate change impacts in supplier countries [38].

5. Impact on domestic production and policy. According to a 2023 report by the European Commission (EC), maize yields declined by 25%, while olive oil production fell by nearly 40% during the 2022/23 season, creating a need for imports (for example, from Ukraine) to offset supply shortages [39]. This issue can also be examined across individual European countries (Table 7.2).

Table 7.2

Threats and losses for EU countries

Country	Threat	Yield losses
Romania, Bulgaria, Hungary, Slovakia	Drought / heat	Up to 24% (Bulgaria), 25% (Hungary), 29% (Romania), and 11% (Slovakia) [40; 41]
Hungary, Romania, Bulgaria	Water scarcity, extreme heat	Significantly reduced crop biomass [42]
The Netherlands, Belgium, France, Germany, the United Kingdom	Dry spring of 2025	Risks of losses of 20–30% [33]
Lithuania, Latvia, Estonia, Poland	Dry growing season of 2023	32% of the territory in Lithuania and 10% in Latvia [34].
Greece	Heat and drought in 2024	A 90% decline in chestnut yields [43].

According to European Commission forecasts for 2024–2035, a partial increase in the yields of cereals and oilseed crops is expected due to innovative methods and improved soil health; however, climate risks will remain significant, especially in southern EU countries [44; 36].

The examples presented in Table 7.2 demonstrate that EU countries are already suffering from droughts, heatwaves, and water scarcity, which reduce the yields of key crops such as maize, sunflower, cereals, olives, and chestnuts. Southern countries are affected primarily by heat; central and eastern countries by a combination of heat and insufficient moisture; and northern countries by excessive moisture, which complicates cultivation. These data support the authors' view that EU food security is vulnerable, and that countries dependent on imports increasingly turn to regions with high climate risk, thereby increasing instability in the food sector.

6. Hygienic and sanitary security. The European Environment Agency notes that two thirds of EU water bodies are in poor condition; each year, about 20% of EU territory faces water-related problems, and over 30% of the population is exposed to risks due to industrial and agricultural pollution (mercury, pesticides). In addition, approximately 20% of EU territory annually experiences water scarcity (water supply deficits), and around 30% of the EU population suffers from water stress or is at risk due to water shortages or contamination [45]. Moreover, more than 30% of the population faces health risks from industrial and agricultural pollution. In particular, mercury, pesticides, and other toxic substances and chemicals enter water bodies through oil installations, emissions, wastewater discharges, and agricultural runoff [46].

There is another problem: the spread of tropical diseases into atypical regions. Rising temperatures, prolonged warm seasons, and changes in precipitation patterns create favorable conditions for mosquitoes that transmit diseases such as malaria, dengue, chikungunya, West Nile virus, as well as for vectors of tick-borne infections (Lyme disease, tick-borne encephalitis) [47]. In particular, the mosquito *Aedes albopictus* (the Asian tiger mosquito) has already become established in 13 European countries (including Italy, France, Spain, Germany, Greece, and Portugal), facilitating the spread of dengue fever and other diseases in regions where they previously did not occur. The duration of the disease transmission season is increasing, and the likelihood of outbreaks is rising [48]. The EEA also acknowledges that climate-sensitive infectious diseases may begin to spread to northern Europe due to warming and longer vegetation seasons for mosquitoes and ticks [47].

In the context of deepening climate change and the increasing frequency of natural disasters, there is an urgent need for a comprehensive approach to reducing the risks and impacts of these phenomena. The effective combination of climate change mitigation measures and adaptation strategies makes it possible not only to minimize damage to the environment and the economy, but also to enhance the resilience of territories to emerging challenges. Let us consider the key areas of response to climate threats, including the reduction of greenhouse gas emissions, adaptive management of natural resources, the development of early warning systems, community engagement, international cooperation, and support for innovative solutions. Particular attention will be paid to the measures implemented by the European Union in the field of forest fire prevention and response to climate challenges:

Mitigation measures. Reducing greenhouse gas emissions is crucial for slowing climate change and its impacts. This includes the transition to renewable energy sources, improving energy efficiency, and reducing deforestation.

Sustainable forest management. The implementation of practices such as forest thinning, the creation of firebreaks, and the use of fire-resistant tree species can help reduce the risk and severity of wildfires.

Water resource management. Improving water conservation, promoting the protection of water resources, and introducing drought-resistant agricultural practices are essential.

Early warning systems. The development and improvement of early warning systems for droughts and fires can help communities prepare for and respond effectively.

Community engagement. Involving local communities in fire prevention efforts and water resource management is critical to success.

International cooperation. The exchange of best practices, coordinated response, and the provision of financial assistance to vulnerable regions are important for addressing the transboundary nature of these challenges.

Research and innovation. Continued research into drought-resistant crops, fire-resistant building materials, and new water management technologies is vital.

Natural and environmental threats pose real risks to societal functioning, economic development, and political stability. Today, in Europe, these threats are becoming particularly acute, as the continent is densely populated, highly urbanized, and under significant environmental pressure. The EU

seeks not merely to react to these challenges, but to move toward systemic governance of sustainable development by integrating environmental criteria into all areas of policy.

Ensuring environmental security today is a guarantee of survival and competitiveness in the future.

7.3. Socio-economic and political threats to contemporary security

The modern world, as has been repeatedly emphasized, is rapidly globalizing, and this process also applies to problems that are acquiring a global scale. In academic literature, there are numerous approaches to identifying socio-economic and political threats to security. In this section, we attempt to examine these concepts in light of contemporary realities.

By socio-economic threats, we understand the entire set of factors that arise within the social environment (including the economic sphere of societal life) and negatively affect various aspects of the lives of individuals, society, the state, the region, and the world as a whole.

One of the most acute issues is Europe's energy security. Despite relatively optimistic plans, the EU continues to face challenges in guaranteeing energy security. In June 2023, EU member states failed to agree on new rules for reforming the electricity market, which were intended to prevent a recurrence of the 2022 energy crisis and curb the rapid rise in energy prices. The core of the disagreement concerned the continuation of subsidies for coal-fired power plants, whose operation remains crucial for many EU countries. For example, Poland generates around 70% of its electricity from coal and is therefore interested in prolonged support (until 2028) for such power plants. An additional argument in favor of extending subsidies was the fact that stable electricity production in Poland could, if necessary, help support Ukraine with reserve energy supplies. By contrast, a number of countries (such as Austria, Belgium, Germany, and Luxembourg) opposed the continuation of subsidies for coal-fired power plants, arguing that this contradicts the principles of the European Green Deal [49, p. 58].

It should also be noted that Europe cannot abandon Russian oil without causing significant damage to European economies. In September 2025, U.S. President D. Trump urged Europeans to stop purchasing oil from Russia and to exert economic pressure on China [50]. Such a shift is unlikely in the near future, as European countries, amid economic recession, are unable to rapidly replace their fuel supply sources. Germany is particularly dependent on oil:

in 2024, it imported 10.6 million tonnes of oil from Kazakhstan [51]. Between January and July 2025 alone, Kazakhstan increased oil transit to Germany by 38% [52]. Given that these supplies are transported via the Druzhba oil pipeline through the territories of Russia and Ukraine, dependence on Russia nevertheless persists.

Currently, political and economic discourse within the EU increasingly emphasizes the development of renewable energy sources; however, skepticism regarding their reliability is also frequently expressed. The Net-Zero Industry Act adopted in 2024 aims to promote the creation of so-called ‘valleys’, clusters of companies focused on specific clean technologies, in order to strengthen the EU’s industrial and energy resilience [53].

Another important issue is employment in the EU. This problem is linked to a number of factors and events observed in the 21st century. One of the first major blows to European economies was the 2008 crisis, which originated in the United States and spread across almost the entire world. In many EU countries, unemployment rates rose sharply, especially among young people. Significant losses were suffered by the banking sector, construction industry, insurance, and other areas of the economy. In European countries, the share of so-called “precarious” employment increased, in which people are hired without social guarantees or with substantial limitations on them.

The employment situation was also affected by the COVID-19 pandemic, which for a prolonged period altered the functioning of entire sectors of the economy. The strictness of quarantine measures varied significantly across EU countries: in Sweden they were minimal (largely based on voluntary self-restraint), whereas in Italy, France, and Spain citizens were for months prohibited from engaging in almost all everyday activities involving leaving their homes and maintaining social contacts. It should be noted that virtually all EU countries are post-industrial, with the majority of people employed in the service sector, which often relies precisely on social interaction. As a result, between April and June 2020 more than one million Spaniards lost their jobs [54].

Among the sectors most severely affected by the pandemic were tourism, transport (passenger services), hospitality and catering, and the entertainment industry. During the pandemic, enterprises and workers in the informal (shadow) economy were hit particularly hard. This sector is characterized by ‘low productivity, limited savings and investment, and minimal capital accumulation, which makes it especially vulnerable to

financial and economic shocks' [55, p. 65]. In addition, informally employed workers often had no entitlement to assistance (at least not to the same extent and under the same conditions as formally employed workers).

Contemporary employment problems in Europe are also linked to rising energy prices and the closure (or the prospect of closure) of a number of industrial enterprises. For instance, at the end of 2024, Volkswagen AG announced plans to shut down at least three plants, cut thousands of jobs, and reduce wages for tens of thousands of German employees [56]. The situation is further aggravated by competition from Chinese manufacturers.

The demographic crisis is another challenge facing the entire European continent. Throughout the 20th century, ongoing urbanization led to the widespread formation of the nuclear family (parents and children only) with a small number of children, while family size has continued to decline. At the same time, life expectancy has increased significantly, resulting in a growing share of elderly people. All of this leads to an 'inversion' of the demographic pyramid: fewer young people and more older citizens. This trend is observed in virtually all developed countries: almost all European countries (not only EU members), as well as Japan, South Korea, and others, are experiencing demographic crisis. This increases pressure on state budgets, as ever greater resources must be allocated to pensions and healthcare. At the same time, countries face the risk of declining demand for professions related to childhood and youth (primarily in the education and childcare systems). The crisis is also likely to affect producers of goods for children and young people.

In the coming decades, the trend toward declining fertility is likely to persist. In 2023, the total fertility rate in the EU stood at 1.38. Bulgaria recorded the highest rate (1.81), while Malta had the lowest (1.06) [57]. European countries are undergoing ongoing social transformations; in particular, the number of people who consciously choose not to form a family and/or have children is increasing. In contemporary sociological discourse, the terms 'singleton' and 'childfree' are widely used. These are often residents of large metropolitan areas with higher education and well-paid jobs, who focus on self-development and are not strong advocates of preserving traditional values. Thus, a clear trend can be observed: 'the more educated a person is, the more mobile they are in life, the more effort they invest in further improvement, self-development, and self-realization, and the less they adhere to traditions, socially accepted norms, and values' [58, p. 24].

Despite the fact that conservative-minded commentators and even some researchers view this as a challenge, we proceed from the assumption that every individual has the right to make their own choices. At the same time, the task of European institutions and national governments is to facilitate as much as possible the transition to a new social reality. Thus, the workforce in future Europe is likely to be smaller in size, but more highly educated.

When discussing declining fertility rates and the simultaneous decrease in the share of the indigenous population in European countries, it is impossible to ignore the issue of migration. This phenomenon has been known to humanity since ancient times. People have moved to other places in search of better living conditions and employment, or to escape natural disasters, religious and political persecution, and other threats. European countries are a major destination for migrants from various parts of the world. Under current socio-political conditions, the EU recognizes the need to increase the number of labor migrants within its territory and emphasizes the necessity of pursuing a more selective policy regarding the admission of third-country nationals to national labor markets [59, p. 320].

At the same time, it should be noted that mass migration can place pressure on healthcare systems, secondary and higher education, social welfare, and housing and public utilities. Countries receiving large numbers of migrants may lack sufficient resources to provide services at an adequate level.

When examining migration to the EU, several conceptual points should be highlighted:

1. Migration to EU countries serves different purposes: educational, labor-related, family reunification, social, political, and others.
2. The majority of migrants come from Africa and the Middle East and represent cultures that are significantly different from European ones.
3. Migrants are distributed very unevenly across EU countries: some states receive large numbers (Italy, France, Germany), while others receive very few (Hungary, Slovakia).
4. Migrants are employed across all sectors of the economy, but predominantly in construction, services, logistics, transport, and related fields.
5. Alongside legal migration, illegal migration exists, which poses a significant threat to security.

Migrants (and their children) and native EU residents differ, among other things, in their access to quality education. Thus, 29% of students whose

parents were born abroad lack basic reading skills, whereas among children whose parents were born in the EU this share is 18% [60, p. 4]. According to a number of other educational indicators, children of migrants also differ from children of the native population. This gap may lead to the ghettoization and radicalization of young people of foreign origin. Socio-cultural conflicts are not uncommon in cases where attempts by society, the state, or European institutions to ensure the integration of migrants into the social, economic, and political environment prove unsuccessful, in particular due to migrants' rejection of Western cultural models. Radical Islamism 'suggests' a violent path of struggle to such individuals, which constitutes a precondition for terrorism. This issue will be addressed below.

Radicalization is often driven by the subjective perception of deprivation, injustice, and a lack of social mobility [61]. Representatives of the younger generation frequently perceive the modern world as unjust; for example, there is a significant gap between young people's incomes and housing costs. This is especially evident in the case of migrant families which, as noted above, tend to live in poorer conditions compared to the native population. This exacerbates feelings of loneliness and isolation, including a distorted self-perception and uncertainty about one's involvement in societal life and belonging to its core structures [62, p. 99]. Such individuals are often drawn into extremist and terrorist activities.

Terror in Europe is not a new phenomenon. The 1914 assassination in Sarajevo became the trigger for the outbreak of the First World War. During the Cold War, the 'Red Brigades' operated in Italy – a clandestine radical organization focused on assassinations of officials, politicians, and members of the military. In West Germany (the FRG), the "Red Army Faction" played a significant destabilizing role and was responsible for a series of murders, robberies, and kidnappings. National movements also frequently assumed the form of terrorist organizations, such as ETA in Spain and the IRA in the United Kingdom.

However, by the early 2000s, almost all left-wing radical organizations had either been dismantled or transformed into marginal groups that no longer posed a serious threat. At the same time, a new challenge emerged for European civilization: Islamist terrorism. In our view, a fundamentally new era in the history of terrorism and counterterrorism began in 2001, following the attacks in New York and Washington. From that point on, the international community became fully aware of the global nature of terrorism

(although international links between terrorist groups had already been observed in previous decades).

In 2003, the European Union adopted the European Security Strategy, which identified terrorism as one of the greatest threats to European security. In particular, the document stated that Europe is not only a target but also a base for terrorists. It emphasized the need for close cooperation among all organizations responsible for the security of the Member States and the judicial system. The European Security Strategy was the result of many years of efforts to strengthen and improve the security situation. The Declaration on Combating Terrorism, adopted by the European Council in 2004, was a response to the terrorist attacks in Madrid in the same year. The adopted document summarized previously initiated counterterrorism measures and outlined directions for further action [63, p. 69].

The already mentioned series of terrorist attacks in Madrid (train bombings in March 2004) became one of the first events in the long history of Islamist terrorism in Europe. In 2005, a series of attacks took place in London, and in 2015 several attacks with major consequences occurred in Paris, including the attack on the editorial office of the magazine *Charlie Hebdo*. Over the past ten years, numerous attacks have taken place, carried out mainly by radicalized citizens: at Brussels Airport (2016), in Nice (2016), and in Vienna (2020). At the same time, another trend can be observed: terrorist attacks may also be carried out by representatives of right-wing movements or lone extremists who support anti-immigrant ideas. Examples include A. Breivik's attack on a youth camp in Norway (2011) and T. Rathjen's attack on a café in Germany (2020).

It is also important to mention left-wing extremist movements. As of 2024, left-wing radicals and anarchists focused on both international and local socio-political issues. Left-wing radical propaganda appealed to ideas of antifascism, anti-imperialism, anti-capitalism, anti-colonialism, and related ideologies. Support for Palestinians and Kurds is widespread among left-wing radicals. Left-wing extremists also oppose NATO and the EU [64, pp. 46–47]. At the same time, in recent years no large-scale successful terrorist attacks carried out by supporters of the above-mentioned ideological currents have been recorded. As noted above, these groups are marginal and do not pose a significant threat.

In recent years, tensions have intensified between the European supranational center and the political leaders of individual countries. The activities of the European Commission and the European Parliament are not

always supported by political leaders in Hungary, Slovakia, Poland, and other states. For example, Hungarian Prime Minister V. Orbán has consistently criticized the “Green Deal,” arguing that its development did not take industrial interests into account. He also emphasizes that the abandonment of cheap Russian energy sources has contributed to crises in the European economy [65]. At the same time, Orbán is skeptical about providing aid to Ukraine, a stance shared by Slovak Prime Minister R. Fico.

A widely held position in European political discourse is the call for a reduction in aid to Ukraine. For instance, Czech opposition leader A. Babiš stated that the supply of shells to Ukraine under the ‘Czech initiative’ costs taxpayers too much [66]. This disagreement is compounded by mismatches between the EU-wide and national levels regarding migration, sanctions, judicial policies, and more. Prospects for the accession of other countries, including Ukraine, to the EU also hinder unity: political elites in several states are fundamentally opposed to the enlargement of the organization, as it would exacerbate existing crises.

Thus, the social, economic, and political dimensions of crises in contemporary Europe are important factors that must be taken into account when developing and implementing policies at both the national and international levels.

References

1. Касьянова, Н. В., Волощук, Д. В., Комісар, М. Ю. (2025). Вплив глобалізації на інноваційний розвиток України. Сталий розвиток економіки. № 2 (53). С. 197–205. <https://doi.org/10.32782/2308-1988/2025-53-27>
2. Жукова, О. Ю. (2024). Вплив глобалізаційних процесів у світовій економіці на промислову діяльність. Вісник ХНТУ. № 4. С. 463–470. <https://doi.org/10.35546/kntu2078-4481.2024.4.63>
3. Ajide, F. M., Osinubi, T. T., Dada, J. T. (2021). Economic Globalization, Entrepreneurship, and Inclusive Growth in Africa. *Journal of Economic Integration*. Vol. 36, No. 4. P. 689–717. <https://doi.org/10.11130/jei.2021.36.4.689>
4. Swadźba, S. (2024). Slowbalizacja czy deglobalizacja? *Ekonomia Międzynarodowa*. No. 45. S. 5–21. <https://doi.org/10.18778/2082-4440.45.01>

5. Nazia, A. (2018). Role of transnational corporations (TNCs) in the world economy – an evaluation. *Journal of Business and Society*. Vol. 9. P. 139–153.

6. Горник, В. Г., Масик-Бесова, В. З., Євмешкіна, О. Л. (2023). Лобістська діяльність в системі державного управління. Держава та регіони. Серія: Публічне управління і адміністрування. № 3 (81). С. 110–115. <https://doi.org/10.32782/1813-3401.2023.3.17>

7. Myskiv, G. (2025). Digital nomads as a contemporary trend in the global labor market. *Economics, Finance and Management Review*. Issue 2 (22). P. 94–108. <https://doi.org/10.36690/2674-5208-2025-2-94-108>

8. Webb, A. K. (2024). Digital nomadism and the challenge to social citizenship. *Global Policy*. Vol. 15. Issue 2. P. 301–313. <https://doi.org/10.1111/1758-5899.13377>

9. Vizjak, M., Perić Kaselj, M. (2024). Digital nomads: the whole world as a global office. *Journal of Process Management and New Technologies*. Vol. 12, Issue 1-2. P. 31–40. <https://doi.org/10.5937/jpmnt12-49306>

10. Сай, Л. П., Назаренко, В. Л., Осередчук, А. М. (2023). Глобалізаційні процеси і участь у них ЄС. Економіка та суспільство. Вип. 50. <https://doi.org/10.32782/2524-0072/2023-50-18>

11. Отенко, І., Птащенко, О. (2020). Тенденції розвитку високотехнологічної сфери в умовах глобалізації. Вісник Тернопільського національного економічного університету. № 4. С. 65–76. <https://doi.org/10.35774/visnyk2020.04.065>

12. Бабкін, В. О. (2018). Глобалізаційні культурні процеси та їх вплив на функціональне призначення національної культури. Мистецтвознавчі записки. Вип. 33. С. 55–62.

13. Amin, T. (2024). Globalization and cultural homogenization: a critical examination. *Kashf Journal of Multidisciplinary Research*. Vol. 1. No. 3. P. 10–20.

14. Грачевська, Т., Гірман, А. (2023). Проблеми та перспективи реформування ООН: позиція України. Геополітика України: історія і сучасність. Вип. 1 (30). С. 56–66. [https://doi.org/10.24144/2078-1431.2023.1\(30\).56-66](https://doi.org/10.24144/2078-1431.2023.1(30).56-66)

15. Peace and Security. United Nations Security Council. Available at: <https://main.un.org/securitycouncil/en>

16. Гамова, О. В. (2021). Міжнародний валютний фонд на сучасному етапі. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове

господарство. Вип. 38. С. 17–21. <https://doi.org/10.32782/2413-9971/2021-38-3>

17. Бублик, Є.О. (2024). Актуальні питання реформування політик і практик МВФ та Світового банку. Економіка та суспільство. Вип. 64. <https://doi.org/10.32782/2524-0072/2024-64-41>

18. Osborbe, M. (2024). Mexico's bloodiest election in modern history set to give first woman president. Sky News. Available at: <https://news.sky.com/story/mexicos-bloodiest-election-in-modern-history-set-to-give-first-woman-president-13146748>

19. Ratsimbaharison, A.M., Bongang, B.L. (2022). Understanding the Durability of the Paul Biya Regime in Cameroon: A Micro-Level Approach Using Afrobarometer's Round 7 National Survey. Current Research Journal of Social Sciences. Vol. 05, No. (2). P. 83–95.

20. Шуліка, А. А. (2018). Організаційні особливості та специфіка практичної діяльності антиглобалістських політичних рухів. Регіональні студії. № 13. С. 36–40.

21. Water investment key to averting global conflict Surge (2024). Vision of Humanity. Available at: https://www.visionofhumanity.org/wp-content/uploads/2024/10/Ecological-Threat-Report-2024-PR-Embargoed-301024.pdf?utm_source

22. Ecological Threat Report 2024. Available at: https://www.economicsandpeace.org/wp-content/uploads/2024/10/ETR-2024-web.pdf?utm_source

23. Ecological Threat Report 2023. Available at: https://www.economicsandpeace.org/wp-content/uploads/2023/12/ETR-2023-web.pdf?utm_source

24. Economic and financial impacts of nature degradation and biodiversity loss (2024). European Central Bank. Available at: https://www.ecb.europa.eu/press/economic-bulletin/articles/2024/html/ecb.ebart202406_02~ae87ac450e.en.html?utm_source

25. Press release: IPBES report reveals options for achieving the transformative change urgently needed to halt biodiversity collapse (2025). Workshops for biodiversity. Available at: https://www.ateliersbiodiversite.org/en/post/press-release-ipbes-report-reveals-options-for-achieving-the-transformative-change-urgently-needed?utm_source

26. New IPBES reports reveal huge economic and business opportunities for accelerating biodiversity action (2024). European Commission. Available at: https://environment.ec.europa.eu/news/ipbes-reports-reveal-huge-opportunities-biodiversity-action-2024-12-18_en?utm_source

27. Biodiversity hit to economies estimated at up to \$25tn a year in landmark report (2024). Financial Times. Available at: https://www.ft.com/content/fed37e59-1f36-453a-a9b1-70f94c8b24f9?utm_source

28. Economic losses from weather- and climate-related extremes in Europe. European Environment Agency (2025). Available at: https://www.eea.europa.eu/en/analysis/indicators/economic-losses-from-climate-related?utm_source

29. Nature degradation could cause a 12% loss to UK GDP (2024). Environmental Change Institute. Available at: https://www.eci.ox.ac.uk/news/nature-degradation-could-cause-12-loss-uk-gdp?utm_source

30. The economic impact of floods. European Central Bank (2025). Available at: https://www.ecb.europa.eu/press/economic-bulletin/focus/2025/html/ecb.ebbox202501_04~ff5de054b8.en.html?utm_source

31. Urgent action needed to reverse soil degradation in Europe. European Commission (2024). Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/urgent-action-needed-reverse-soil-degradation-europe-2024-10-22_en?utm_source

32. Abnett, A. (2025). Extreme weather costs EU farmers 28 billion euros a year, EU says. Reuters. Available at: https://www.reuters.com/sustainability/cop/extreme-weather-costs-eu-farmers-28-billion-euros-year-eu-says-2025-05-20/?utm_source

33. ‘It’s a critical time’: European farmers struggle through driest spring in a century (2025). The Guardian. Available at: https://www.theguardian.com/environment/2025/may/22/its-a-critical-time-european-farmers-struggle-through-driest-spring-in-a-century?utm_source

34. Drought impact on ecosystems in Europe (2025). European Environment Agency. Available at: https://www.eea.europa.eu/en/analysis/indicators/drought-impact-on-ecosystems-in-europe?utm_source

35. Global climate change impacts and the supply of agricultural commodities to Europe (2021). European Environment Agency. Available at: https://www.eea.europa.eu/publications/global-climate-change-impacts-and/global-climate-change-impacts-and?utm_source
36. Agriculture. Climate Adapt. Available at: <https://climate-adapt.eea.europa.eu/en/eu-adaptation-policy/sector-policies/agriculture>
37. EU's 'chocolate crisis' worsened by climate breakdown, researchers warn (2025). The Guardian. Available at: https://www.theguardian.com/environment/2025/may/21/eu-chocolate-climate-breakdown-crisis-report?utm_source
38. Ercin, E., Veldkamp, T.I.E., Hunink, J. (2021). Cross-border climate vulnerabilities of the European Union to drought. Nature communications. Available at: https://www.nature.com/articles/s41467-021-23584-0?utm_source=twitter&utm_medium=social&utm_content=organic&utm_campaign=NGMT_USG_JC01_GL_NRJournals
39. Short-term outlook report: war in Ukraine continues to impact EU farmers (2023). European Commission. Available at: https://agriculture.ec.europa.eu/media/news/short-term-outlook-report-war-ukraine-continues-impact-eu-farmers-2023-03-30_en?utm_source
40. Ozalp, O. (2024). Crop monitoring in Europe August 2024. JRC MARS Bulletin. Vol. 32. No. 8. 26 August 2024. 42 p.
41. Worsened yield outlook for grain maize and sunflowers (2024). European Commission. Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/worsened-yield-outlook-grain-maize-and-sunflowers-2024-09-23_en?utm_source
42. Persistent droughts: critical water shortages and crops threatened (2024). European Commission. Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/persistent-droughts-critical-water-shortages-and-crops-threatened-2024-07-31_en?utm_source
43. Papadimas, L., Avramidis, A. (2024). Greece's chestnut harvest set to shrink, hit by drought and heat. Reuters. Available at: https://www.reuters.com/business/environment/greeces-chestnut-harvest-set-shrink-hit-by-drought-heat-2024-10-24/?utm_source
44. EU agricultural outlook 2024-35: A resilient sector adapts to climate change, sustainability concerns, and shifting consumer demand (2024). European Commission. Available at: <https://agriculture.ec.europa.eu/media/news/eu-agricultural-outlook-2024->

[35-resilient-sector-adapts-climate-change-sustainability-concerns-and-2024-12-11_en?utm_source](#)

45. Almost two-thirds of EU water in bad condition, report shows (2024). Financial Times. Available at: https://www.ft.com/content/cf7b8e4e-e950-45ca-8ada-ea7f7d0c0ffd?utm_source

46. Pollution, over-use and climate change threaten water resilience in Europe. European Environment Agency. Available at: https://www.eea.europa.eu/en/newsroom/news/state-of-water?utm_source

47. Heatwaves, spread of infectious diseases due to climate change growing health threats to Europeans (2022). European Environment Agency. Available at: https://www.eea.europa.eu/en/newsroom/news/heatwaves-spread-infectious-diseases?utm_source

48. Mosquito-borne diseases spreading in Europe due to climate crisis, says expert (2024). The Guardian. Available at: https://www.theguardian.com/environment/2024/apr/25/mosquito-borne-diseases-spreading-in-europe-due-to-climate-crisis-says-expert?utm_source

49. Кукуруз, О. В., Батанова, Н. М. (2023). Енергетична політика ЄС: реформування та проблеми реалізації в контексті геополітичних викликів. Політикус. Вип. 5. С. 55–60. <https://doi.org/10.24195/2414-9616.2023-5.8>

50. Treene, A., Ataman, J. (2025). Trump pushes Europe to stop buying Russian oil and up pressure on China in effort to end Ukraine war. CNN. Available at: <https://edition.cnn.com/2025/09/04/politics/ukraine-war-trump-security-guarantees>

51. Shayakhmetova, Zh. (2025). Kazakhstan Deepens Ties with Germany, Announces Plans to Increase Oil Transportation. The Astana Times. Available at: <https://astanatimes.com/2025/05/kazakhstan-deepens-ties-with-germany-announces-plans-to-increase-oil-transportation/>

52. Волокіта, В. (2025). Експорт нафти з Казахстану до Німеччини зріс майже на 40%. Економічна правда. Available at: <https://epravda.com.ua/energetika/eksport-nafti-z-kazahstanu-do-nimechchiny-zris-na-38-810228/>

53. EU Net-Zero Industry Act. EUR-lex. Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/eu-net-zero-industry-act.html>

54. Pollet, M. (2020). Coronavirus crisis: A million people lose their jobs in Spain in just three months. Euronews. Available at: <https://www.euronews.com/2020/07/29/coronavirus-crisis-a-million-people-lose-their-jobs-in-spain-in-just-three-months>

55. Длугопольська, Т., Хіта, М. (2022). Вплив пандемії Covid-19 на міжнародний ринок праці. Вісник економіки. Вип. 1. С. 54–70. <https://doi.org/10.35774/visnyk2022.01.054>
56. VW Seeks Unprecedented Plant Closings as Auto Crisis Deepens (2024). Bloomberg. Available at: <https://www.bloomberg.com/news/articles/2024-10-28/vw-eyes-closing-three-german-factories-in-cost-cutting-push>
57. Fertility statistics. Eurostat. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Fertility_statistics
58. Малога, М. (2019). Childfree: новий стиль життя та виклик для українського суспільства. Український педагогічний журнал. № 2. С. 21–28. <https://doi.org/10.32405/2411-1317-2019-2-21-28>
59. Денисюк, П. Д. (2021). Основні тенденції міграційних процесів країн Європи. Юридичний науковий електронний журнал. № 4. С. 318–321. <https://doi.org/10.32782/2524-0374/2021-4/77>
60. Integration of migrant children (2023). European Parliamentary Research Service. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754601/EPRS_BRI\(2023\)754601_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754601/EPRS_BRI(2023)754601_EN.pdf)
61. García López, M. A., Pašić, L. (2018). Youth work against violent radicalisation. Theory, concepts and primary prevention in practice. Council of Europe. Available at: <https://pjp-eu.coe.int/documents/42128013/47261953/YW-against-radicalisation-web.pdf/90a7569d-182d-0b0c-ce5d-9a0fe111ec91>
62. Шевчук, Я. (2024). Превенція радикалізації та насильницького екстремізму як інструмент запобігання тероризму: європейський досвід і шляхи його імплементації в Україні. Право України. № 12. С. 95–114.
63. Чернадчук, Т. О., Березовська, В. О. (2022). Політика Європейського Союзу щодо боротьби з тероризмом: аналіз законодавства Європейського Союзу та деяких національних антитерористичних програм. Правова держава. Вип. 48. С. 66–76. <https://doi.org/10.18524/2411-2054.2022.48.267964>
64. European Union terrorism situation and trend report 2025. Publications Office of the European Union, Luxembourg. Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

65. Viktor Orbán and Ursula von der Leyen clash in fiery debate at European Parliament (2024). Euronews. Available at: <https://www.euronews.com/my-europe/2024/10/09/viktor-orban-and-ursula-von-der-leyen-clash-in-fiery-debate-at-european-parliament>

66. Czech ammo lifeline for Ukraine comes under fire at home (2025). Politico. Available at: <https://www.politico.eu/article/czech-republic-andrej-babis-ammunition-war-in-ukraine/>

Chapter 8

Security challenges of the 21st century: harmonization of global and national interests (L. Shchekhovska, A. Zahorodnia)

In the 21st century, the global security architecture is undergoing fundamental transformations under the influence of globalization, technological progress, and new forms of conflict. Traditional threats – armed conflicts, terrorism, and nuclear confrontation – have undergone fundamental transformation, while the digital era has spawned entirely novel challenges: cyber threats, information wars, and the use of artificial intelligence for military purposes.

A defining characteristic of the contemporary era is the systemic interdependence of threats and their cascading impact. A fundamental tension has emerged between the transnational scope of contemporary challenges and the predominantly state-centric response mechanisms. There is an observable transformation in the very concept of security from a military-political understanding to a comprehensive approach that encompasses economic, environmental, informational, and technological dimensions. Exploring the mechanisms for harmonizing global security imperatives with the national interests of states is the purpose of this chapter.

8.1. Key security challenges of the present

Analyzing contemporary security challenges necessitates a systemic approach that considers their evolutionary nature and interconnectedness. The methodological foundation of this typology rests on the integration of time-based, scale-based, and structural criteria.

The time-based criterion distinguishes traditional threats that have acquired new forms under the influence of technology from fundamentally new challenges of the digital era. The scale criterion highlights systemic

cross-border risks that affect the stability of the international system. The structural approach accounts for the hybrid nature of modern challenges – a combination of different instruments of influence and the blurring of the boundaries between internal and external threats.

This methodological framework provides analytical coherence to the diversity of challenges and reveals the logic of their interaction, which is essential for formulating effective countermeasures aimed at countering them and harmonizing national and global security interests.

1. Traditional threats in a new format. A central obstacle to contemporary counterterrorism efforts lies in the absence of a universally accepted definition of the term '*terrorism*'. Although the international community has developed 19 specialized counterterrorism conventions under the auspices of the UN, each of them addresses only specific aspects of terrorist activity. This fragmentation stems from profound political and ideological cleavages among states regarding the qualification of acts as terrorist.

In Ukrainian legislation, terrorism is defined as socially dangerous activity involving the deliberate use of violence with the aim of violating public safety, intimidating the population, or influencing decision-making by public authorities in order to achieve political, religious, or ideological goals [1].

Terrorism has undergone a qualitative metamorphosis in the 21st century, morphing from territorially bounded insurgencies into a globalized threat that integrates advanced technologies. Modern terrorist structures operate autonomously, using decentralized platforms and encrypted communication networks. Traditional kinetic violence has been augmented by cybercrime, psychological operations, and information propaganda.

Technological capabilities have become integral to the terrorist toolkit. Unmanned aerial vehicles have emerged as a weapon of choice for asymmetric warfare due to their accessibility and mobility. Their use for delivering explosives and attacking infrastructure has been documented in Syria, Iraq, Ukraine, and the Philippines.

Cryptocurrencies have provided terrorist groups with new channels to evade sanctions and transfer funds. ISIS units actively used Bitcoin wallets to receive donations, while banned organizations conducted fundraising through cryptocurrency exchanges [3]. Under conditions of weak global regulation, such operations remain practically untraceable.

The darknet functions as a hidden segment of the Internet, providing anonymous access to recruitment forums, bomb-making instructions, and the formation of international terrorist networks [2].

Recent cases from 2024–2025 confirm these threats. In Europe, a supply network providing drone components to Hezbollah was exposed, and in Pakistan, TTP (Tehreek-i-Taliban Pakistan) carried out an attack using a remote-controlled quadcopter. FATF reported an intensification of fundraising through social media and cryptocurrencies [4].

Terrorism in the 21st century has transformed from a local issue into a global phenomenon of technological adaptation, requiring a rethinking of traditional approaches to ensuring national and international security.

Nuclear non-proliferation has re-emerged as a paramount security concern to global security. Despite rhetorical commitments under the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) to nuclear disarmament, profound divergences over implementation pathways produce deepening political fractures. A dual paradox characterizes the current moment: declaratory aspirations for a nuclear-free world belie the de facto expansion of nuclear capabilities.

The officially recognized nuclear states under the NPT advocate a gradual and controlled disarmament process, whereas supporters of the Treaty on the Prohibition of Nuclear Weapons call for an immediate renunciation of nuclear weapons as an instrument incompatible with international humanitarian law. This contradiction is intensified by heightened geopolitical confrontation.

Current developments demonstrate three strategic trends: the strengthening of nuclear arsenals by existing nuclear states, the potential emergence of new “threshold” nuclear actors, and the erosion of trust in arms-control institutions. Russia’s development of advanced nuclear systems, the collapse of the Intermediate-Range Nuclear Forces Treaty, and the United Kingdom’s decision to increase its limit of nuclear warheads indicate a de facto departure from the principles of arsenal reductions.

The situation around Iran has escalated after its gradual withdrawal from the obligations of the Joint Comprehensive Plan of Action and its increased uranium enrichment to levels suitable for producing nuclear weapons [6]. Regional tensions have highlighted that even suspicion of possessing a nuclear program can become a trigger for preemptive military action.

A particular threat is posed by the possible deployment of Russian tactical nuclear warheads in Belarus [7], which violates the spirit of the NPT

and undermines the foundations of the nuclear deterrence regime in Europe. Meanwhile, North Korea's nuclear activity is increasing, stimulating debates in South Korea and Japan about the potential creation of their own nuclear arsenals.

Negotiations on a new strategic arms-control agreement between the United States and Russia have effectively been frozen due to the conflict in Ukraine [5]. In this context, the world is entering a phase of renewed nuclear risk, in which states strategically employ the “nuclear shadow” as an instrument of political pressure. This underscores the need to update control mechanisms and prevent regional conflicts from escalating into global nuclear catastrophes.

2. New Challenges of the Digital Age. *Hybrid threats* have ascended to the forefront of the global security agenda. Consensus is emerging regarding the imperative to manage hybrid threats among academic experts, practitioners, and key international institutions, including NATO and the European Union. Despite persistent definitional ambiguity and the absence of conceptual convergence of “hybrid threats”, it is appropriate to examine the approaches developed by leading research centers (Table 8.1).

The European Centre of Excellence for Countering Hybrid Threats in Helsinki characterizes hybrid threats as coordinated and synchronized activities deliberately directed at systemic vulnerabilities of democratic states and institutions through a wide range of instruments – political, economic, military, civilian, and informational. Such activities characteristically operate below the threshold of detection and attribution, as well as at the intersection of states of war and peace, which enables influence on decision-making processes at the local, regional, national, and institutional levels.

In parallel, the International Institute for Strategic Studies (IISS) defines hybrid warfare as the use of military and non-military instruments within an integrated campaign aimed at achieving surprise, seizing the initiative, and gaining psychological and physical advantages through diplomatic means, sophisticated information and cyber operations, covert military and intelligence activities, and economic pressure [8].

In the Ukrainian legal and regulatory framework, hybrid-type threats are defined as a category of national security threats whose implementation generates a synergistic and cascading effect through the simultaneous use of combined methods of influence that often have a concealed nature or are disguised as other processes within the legal field (Decree of the President of Ukraine of 27 September 2021, No. 479/2021).

Table 8.1

Comparative analysis of the implementation of hybrid threats*

Country	Key mechanisms	Impact modality	Consequences
Ukraine (2014–present)	Proxy forces, cyberattacks, disinformation, blockades	Complex hybrid pressure	Undermining sovereignty, escalation into full-scale war
Estonia (2007)	Cyberattack on government agencies	Cyber operation	Disruption of infrastructure functioning
United States (2016 and 2020 elections)	Information campaigns, fake news, cyberattacks	Political destabilization	Loss of confidence in the electoral process
United Kingdom (Brexit, 2016)	Manipulation on social media, fake news, information pressure	Social polarization	Impact on democratic expression of will
Lithuania, Poland, Latvia (2021–2022)	Migration weapon, propaganda	Border destabilization	Humanitarian and political crisis
Syria (2011–2025)	Proxy forces, propaganda, fake news, humanitarian blockade	Hybrid multilateral warfare	Prolongation of the conflict, delegitimization of international law

* Source: compiled by the authors based on: [8–12]

It is important to emphasize that in the 21st century hybrid threats have become a key element in the transformation of the international security environment. Their distinctive features include their cross-sectoral nature, complex structure, multichannel influence, and inherent difficulty of detection and response.

The analysis of the presented cases demonstrates that hybrid threats are extremely flexible and adaptive forms of influence that allow aggressors to achieve strategic objectives without formally declaring war. They effectively leverage modern technologies, the media environment, social divisions, and political vulnerabilities of democratic systems. Therefore, modern security strategies must take these aspects into account by strengthening resilience to information attacks, cyber threats, and subversive activities, as well as by developing legal and technical mechanisms for identifying and countering multi-vector hybrid pressure.

In the 21st century, *cybersecurity* has evolved from a technical ancillary concern into a cornerstone of national security, economic stability, and societal trust. Within an increasingly interconnected and digitized landscape, cyber threats have acquired a systemic dimension, amplified by geopolitical friction, technological interdependence, and uneven development of regulatory mechanisms.

According to the World Economic Forum's report *Global Cybersecurity Outlook 2025*, the contemporary digital environment is characterized by high complexity, which complicates effective risk management [11]. Key drivers of this complexity include: geopolitical instability, which intensifies cyber espionage and sabotage; vulnerabilities within global supply chains, particularly due to third-party software; rapid implementation of innovative technologies without adequate cybersecurity assessments; a critical shortage of qualified specialists reported by two-thirds of organizations; and regulatory fragmentation, which 69% of organizations consider overly burdensome.

Artificial intelligence poses distinct cybersecurity challenges. In 2025, 66% of organizations view AI as the technology with the greatest impact on cybersecurity, yet only 37% have proper procedures for evaluating the security of AI solutions prior to deployment [11]. This creates significant vulnerability vectors: generative AI is actively used for large-scale phishing attacks and deepfake production; incidents of voice and video impersonation of executives for financial fraud are increasing; platforms such as Cybercrime-as-a-Service are expanding access to criminal tools.

Cyberattacks are increasingly targeting operational technologies of critical infrastructure. In 2024, the largest IT failure in history occurred, paralyzing banks, airlines, and hospitals in more than 20 countries, while cyberattacks on water treatment facilities and energy infrastructure demonstrated the potential threat to population life-support systems [11]. Cyberattacks on satellites, subsea cables, and communication facilities have become routine elements of armed conflicts, including in Ukraine.

The global cyber landscape of the 21st century demonstrates a clear evolution from traditional cybercrime to state-organized campaigns, characterized by increasing attack sophistication and geopolitical impact. The analysis of leading cases reveals systemic transformations in the nature of cyber threats (Table 8.2).

The experiences of Ukraine, the United States, and Israel demonstrate that cyber threats have transformed into a strategic form of modern warfare,

characterized by the combination of cyberattacks with informational influence, the transnational nature of threats, and the blurring of boundaries between war and peace, as well as between state and non-state actors. Cybersecurity has evolved from a paradigm of local responsibility into a global collective challenge, since the vulnerabilities of individual actors in the digital space create cascading effects that threaten the stability of the entire international cyber infrastructure.

Table 8.2

Cybersecurity Cases of Leading Countries*

Country	Types of Threats	Key Attacks / Incidents	Response Strategy
Ukraine	Wiper attacks, cyber espionage, disinformation, fakes, DDoS	NotPetya (2017), Diia, Central Election Commission, energy sector, Telegram fakes	IT Army, CERT-UA, NATO Cyber Centre in Kyiv
United States	Election interference, ransomware, deepfakes	SolarWinds, Colonial Pipeline, Fancy Bear	USCYBERCOM, CIRCIA, public-private partnership
Israel	Cyber espionage, attacks on military infrastructure	Attacks on hospitals, deepfakes during the Hamas conflict	Export of cyber technologies, Israeli CERT

* Sources: [10–12]

Information security and the impact of disinformation. Digital transformation has fundamentally reconfigured the security landscape of the 21st century. Information has acquired a threefold nature, serving concurrently as resource, a vector of influence, and a target of hostile action. The convergence of social networks, artificial intelligence, and surveillance technologies has generated novel threat vectors to national and international security.

The evolution of information security reflects profound changes in the structure of modern conflicts. Whereas previously it focused on the technical protection of data, today it encompasses countering targeted manipulation, cyberattacks, and psychological influence on societies. This shift underscores the transformation of information from a passive object of protection into an active element of geopolitical confrontation.

The systemic use of disinformation technologies has become an integral part of hybrid operations. Fake news, deepfakes, bot networks, and “troll

farms” form an ecosystem of informational influence capable of manipulating public opinion on an unprecedented scale. These technologies deliberately construct alternative realities, deepen social polarization, and undermine trust in democratic institutions.

A notable example is the 2024 incident in which Iranian cyber groups hijacked broadcasting in the UAE, airing an artificially created news program about the conflict between Israel and Hamas. The use of AI to generate a virtual news anchor and synthetic footage illustrates the evolution from distorting facts to creating entirely artificial yet convincing narratives [12].

In parallel, cyberattacks have evolved from isolated acts into a strategic instrument of state policy. The attacks on the tax authority of Costa Rica (2022), the Technion University (2023), DDoS attacks on government portals in Estonia, Lithuania, and the Czech Republic, and cyber operations by Ukrainian hackers demonstrate the institutionalization of cyber conflicts [12].

Artificial intelligence creates unprecedented opportunities for the automated production of content and manipulation of public perception. Bot networks disseminate false messages on a massive scale, creating the illusion of “public opinion.” Structures such as the Internet Research Agency have been conducting systematic disinformation campaigns targeting Ukraine, the United States, and the EU since 2014.

Information security has become a key element of national security. Disinformation, fake news, cyber operations, and the misuse of artificial intelligence are not isolated incidents but indicators of the transformation of conflict into the informational domain. The preservation of the democratic order in the 21st century increasingly depends on societies’ ability to protect their information space.

3. Global Systemic Risks. *Climate change* and *energy security* represent a new paradigm of systemic threats that transcend the traditional division between internal and external risks. The transformation of climate change from an environmental problem into a global security challenge illustrates the interdependence between natural processes, economic systems, and geopolitical stability. The intensification of extreme weather events – abnormal heat waves, droughts, wildfires, and abrupt climate fluctuations – underscores the systemic nature of these threats.

Empirical evidence of climate destabilization is becoming critically important. According to the IMF, 2024 recorded the highest global temperature in the history of observations. “Cooling degree days” increased by 6% compared to 2023 and by 20% relative to the 2000–2020 average. The most vulnerable states were China, India, and the United States. Weather factors accounted for 15% of global energy demand growth, including 20% in electricity and gas sectors [13]. This created a paradox: climate change

stimulates additional fossil fuel consumption, providing half of the increase in global CO₂ emissions in 2024.

Russia's full-scale invasion of Ukraine catalyzed the transformation of energy security into a strategic priority. The European energy market experienced a systemic shock: sanctions and supply reductions pushed gas prices to €345/MWh and oil prices to \$124 per barrel in 2022 [13]. This geopolitical shock accelerated the diversification of energy sources and reinforced the concept of energy autonomy as a key element of national security.

Research confirms a direct relationship between an increased share of carbon-free energy and the achievement of both climate and security objectives. For Europe, a 10% increase in such energy results in a 3% reduction in CO₂ emissions and a 6% decrease in energy imports. Energy efficiency remains a critical factor: over four decades, Europe reduced its energy intensity of GDP by 46.4% [13].

However, current progress is insufficient. Global CO₂ emissions reached a record 36.3 billion tons in 2021, and the pace of decarbonization does not meet the targets of the Paris Agreement [15]. This creates a strategic dilemma: the need to simultaneously ensure energy security and accelerate climate action.

The synergy between climate policy and energy security forms a new paradigm of strategic planning. A shift toward energy efficiency, carbon-free technologies, and carbon taxation creates opportunities to achieve climate goals while strengthening strategic autonomy. In the context of geopolitical turbulence, these approaches are becoming fundamental components of 21st-century national security.

Pandemics and Biosecurity. The convergence of pandemic risks and climate change is shaping a qualitatively new type of systemic threat, transforming biosecurity from a medical issue into a complex national security challenge. Climate factors perform multiple destructive functions: they act as indirect triggers of infectious outbreaks, catalysts of systemic disruptions in healthcare systems, and multipliers of socio-economic instability. Climate change threatens both physical and mental health, undermining social determinants of health through migration flows, resource depletion, and social disintegration.

The COVID-19 pandemic became a turning point in understanding the multidimensionality of biological threats. The outbreak demonstrated the ability of pathogens to paralyze global economic systems, destabilize political structures, and disrupt international supply chains. According to the U.S. National Intelligence Service, the risk of large-scale pandemics is rising

due to the synergy of climate change, urbanization, ecosystem degradation, and increased zoonotic transmission [14].

Climate change functions as a systemic multiplier of biological vulnerability. Extreme weather events, rising temperatures, and natural disasters create conditions for pathogen displacement, the release of isolated infectious agents, and the stimulation of viral mutations. Meanwhile, more than 60% of states lack integrated bio-threat response plans, and early-warning mechanisms remain fragmented.

Particularly problematic is the insufficient integration of biosecurity into climate policy. Despite the recognized link between climate and health, most Nationally Determined Contributions under the Paris Agreement do not include healthcare as a priority. Fewer than 50 countries account for vulnerable population groups or assess long-term health risks related to global warming [14].

The dominant approach to biosecurity – focused on responding to acute crises – ignores the slow, cumulative consequences of climate change. The rise in oncological, respiratory, and mental health disorders resulting from long-term climatic shifts requires fundamentally different strategies. The lack of systemic funding, institutional fragmentation, and weak monitoring critically increase vulnerability to future pandemics.

The transformation of biosecurity into a structural national security challenge demands a fundamental rethinking of state policy, strengthening global solidarity, and creating effective multi-level governance mechanisms. In the context of accelerating climate change, this transformation becomes critically important for the stability of human civilization.

Demographic Challenges and Migration Crises. The modern demographic dichotomy – population aging in highly developed states and the formation of “youth bulges” in developing economies – constitutes one of the fundamental long-term risks of the 21st century. According to the Global Risks Report 2025, countries with a predominantly elderly population, such as Japan, Germany, and South Korea, face labor shortages and systemic pension crises that threaten their economic stability. Conversely, in South Asia and Africa, rapid growth of young populations leads to the exhaustion of employment opportunities and heightened social tension [15].

The growing correlation between demographic trends and migration flows highlights the issue of forced displacement, which is among the leading short-term global risks today. Migration flows from areas affected by conflict, climate change, or economic deprivation encounter limited absorption capacities of host states, provoking local social tensions and fostering radicalization.

Climate factors significantly intensify migration processes: water scarcity, declining agricultural productivity, and extreme weather events trigger new waves of internal and cross-border migration. This creates preconditions for resource conflicts and increases instability in host countries, especially amid rising inequality and eroding trust in public institutions.

8.2. Contradictions between global and national interests

The international system is conventionally understood as an anarchic structure characterized by the absence of overarching authority capable of imposing rules of conduct on states. This structural anarchy engenders persistent security dilemmas, catalyzes arms competition, and limits the possibilities for stable coordination at the global level. Efforts toward international coordination invariably confront trust deficits, resource asymmetry, and the differentiation of interests among state actors. The theoretical foundations of these contradictions lie in the fundamental opposition between the principle of national sovereignty and the concept of global governance. State governments, particularly those of the Global South, systematically perceive attempts to create supranational mechanisms as a potential threat to internal legitimacy and political autonomy. This produces structural tension between international institutions and national governments, which resist external intervention in domestic political processes.

Empirical manifestations of these contradictions are especially evident in the sphere of global security challenges. The COVID-19 pandemic demonstrated the destructive consequences of a lack of coordination: fragmented national responses, competition for medical supplies, and practices of “vaccine nationalism” turned a local problem into a global crisis with more than 7 million casualties. Similarly, the issue of climate change requires coordinated action, yet national economic priorities systematically hinder decisive measures, as illustrated by difficulties in implementing the Paris Agreement. Notable examples include several states’ resistance to an international investigation into the origins of COVID-19 or refusal to participate in global climate initiatives.

It is important to emphasize that conflicts between global and national interests become particularly acute under conditions of great-power competition. The geopolitical rivalry between the United States and China has evolved from trade-technological disputes into a structural geopolitical confrontation manifesting across regions from the South China Sea to Africa.

Parallel to this, Russia’s aggression against Ukraine undermines the established security order in Europe and seeks to promote an alternative

model of sovereign governance in opposition to the principles of the liberal international system.

These geopolitical conflicts directly influence the resolution of global security challenges. Sanctions regimes against Russia, despite being justified in the context of its aggression, complicate cooperation in addressing climate threats and generate energy instability in Europe. The U.S.–China trade war slows the exchange of cybersecurity technologies, creates parallel standards in telecommunications, and undermines global coordination in combating cyberthreats [16].

Another manifestation of global contradictions includes economic wars, trade barriers, and sanctions regimes that function as instruments of power competition. According to the Peterson Institute for International Economics, more than 15,000 different sanctions measures were in effect in 2024, leading to the fragmentation of the global economy and complicating multilateral cooperation [17]. Sanctions imposed on Iran, Russia, or North Korea demonstrate how national strategic interests can undermine universal principles of multilateralism and hinder the resolution of transnational problems.

An equally significant aspect of modern international relations is the growing role of non-state actors, which increasingly compete with traditional states for influence on global politics. Transnational corporations can shape foreign policy through investment mechanisms, lobbying, and control over strategic technologies. Particularly illustrative is the phenomenon of major technology companies that control critical digital infrastructure. Google, Microsoft, and Amazon provide cloud services to government structures, yet may simultaneously restrict access for political reasons.

International organizations, despite formal dependence on member states, increasingly position themselves as carriers of global norms – human rights, sustainable development, climate responsibility. During the pandemic, the WHO attempted to coordinate a global response but faced systematic resistance from states prioritizing national interests over the imperatives of global health. Similarly, UN attempts to create a global cybersecurity system encounter reluctance from countries to disclose information on national cyber capabilities [18].

At the same time, the influence of global non-governmental actors is growing, as they are capable of mobilizing public opinion, shaping the agenda of international summits, and creating alternative sources of legitimacy beyond state authority. Climate activist movements such as *Extinction Rebellion* demonstrate the ability to influence national policies more effectively than traditional international agreements.

Thus, contemporary international politics reflects profound structural contradictions between the logic of autonomous national interest and the need for collective regulation in conditions of global interdependence. These contradictions not only impede the effective resolution of transnational security challenges but also generate new sources of systemic instability, highlighting the need to search for innovative mechanisms to harmonize multi-level interests within the modern international system.

8.3. Mechanisms for harmonizing interests: experience and prospects

The harmonization of global and national security interests has acquired paramount significance in countering the transnational challenges of the 21st century. The systemic interdependence of contemporary threats – from cyberattacks to climate crises – demands coordinated international action capable of transcending structural anarchy while safeguarding sovereign prerogatives.

The system of international organizations, established after the Second World War, remains a central mechanism for aligning security interests; however, its efficacy in confronting contemporary hybrid threats is coming under increasing scrutiny. The United Nations, as a universal platform, provides a normative foundation for collective security, yet the principle of consensus and the veto power impede effective responses to aggression by permanent members of the Security Council. The Russo-Ukrainian conflict vividly illustrates this systemic flaw: the UN's inability to ensure a collective response to violations of fundamental principles of international law undermines trust in universal security mechanisms.

At the same time, specialized UN agencies demonstrate greater effectiveness in sectoral security domains. The World Health Organization coordinated the international response to the COVID-19 pandemic, albeit with limited success due to the dominance of national interests over global solidarity. The International Atomic Energy Agency continues to play a key role in preventing nuclear proliferation, demonstrating the potential of technocratic mechanisms for harmonization in high-tech security sectors [18].

Particularly illustrative is the fight against international terrorism, which, after the events of September 11, 2001, demonstrated the possibility of rapid mobilization of the international community around a common threat. Security Council Resolution 1373 established a robust legal foundation for coordinated counterterrorism measures, while the Counter-Terrorism Committee provided systematic monitoring of their implementation. International cooperation in financial intelligence through

the Financial Action Task Force significantly limited the funding channels of terrorist organizations; however, emerging technological challenges – the use of cryptocurrencies, drones, and darknet networks – require continuous adaptation of these mechanisms.

Against this backdrop, regional organizations exhibit considerably greater flexibility in aligning the security interests of states with similar geopolitical characteristics. The most successful example remains the European Union, which, through qualified majority mechanisms and the principle of subsidiarity, has achieved an unprecedented level of integration in the security sphere. The European response to the energy crisis following Russia's aggression against Ukraine – the REPowerEU plan, coordination of military aid, adoption of comprehensive sanction packages – demonstrates the ability to rapidly align the positions of 27 member states even under crisis conditions when national interests may diverge sharply [18].

NATO, as a military-political alliance, represents a classic example of institutional harmonization of security interests through the mechanism of collective defense. Article 5 of the Washington Treaty established a system of mutual security guarantees that ensured stability in the transatlantic region for decades. At the same time, the alliance's adaptation to new threats – cybercrime, hybrid attacks, terrorism – revealed the necessity of expanding the traditional understanding of collective defense from purely military threats to complex security challenges.

Cybersecurity challenges particularly highlight the difficulties of harmonizing interests in the digital space. The absence of universal norms of cyber behavior allows states to use digital technologies to undermine the sovereignty of other countries while avoiding traditional accountability mechanisms. The Tallinn Manual and the UN Groups of Governmental Experts attempt to create legal frameworks for cyberspace, yet fundamental divergences between democratic and authoritarian regimes regarding the nature of digital sovereignty complicate the achievement of consensus.

In the context of Russian aggression, Ukraine has transformed from a passive object of international policy into an active actor in harmonizing security interests, demonstrating the potential of middle powers to shape international coalitions. The *Crimean Platform*, initiated by the Ukrainian government, united over 60 states around the principle of territorial integrity and the inadmissibility of annexation, creating a new thematic format for coordinating security interests. Ukraine's experience in countering hybrid threats – combining conventional aggression with cybercrime, disinformation, and energy blackmail – establishes new standards of national resilience disseminated through international knowledge-sharing networks.

Contemporary harmonization of security interests increasingly extends beyond traditional interstate diplomacy, encompassing a wide range of non-state actors. Global corporations have become important security agents through control over critical infrastructure and digital platforms. Large technology companies effectively set cybersecurity standards that directly influence national regulation and consumer behavior across jurisdictions.

Digital technologies open fundamentally new opportunities for harmonizing security interests, creating tools capable of radically reducing the transaction costs of international coordination. Blockchain technologies have the potential to provide unprecedented transparency in monitoring compliance with non-proliferation regimes and sanction restrictions. Artificial intelligence can analyze massive datasets for early detection of security threats and optimize the search for mutually beneficial solutions in complex multilateral arms control negotiations.

Simultaneously, fundamentally new types of security institutions are emerging, based on networked organizational principles: flexible membership, thematic specialization, and adaptive governance. International regulatory networks in financial security establish soft standards through expert consensus, effectively bypassing formal ratification procedures. Computer Incident Response Teams function as transnational networks for sharing information on cyber threats, ensuring operational coordination without the bureaucratic procedures of traditional international organizations.

These institutional innovations form the potential for more flexible and adaptive harmonization of security interests, capable of responding promptly to the dynamics of threats. At the same time, they raise fundamental questions of democratic legitimacy and public accountability in new forms of global security governance. Balancing operational efficiency and transparency remains one of the key challenges for the further development of mechanisms for international harmonization of security interests.

Conclusions

This examination of harmonization mechanisms has illuminated fundamental transformations in the 21st-century international system, characterized by the systemic interdependence of threats and their cascading effects on both national and international security. An analysis of the typology of contemporary security challenges has shown an evolution from traditional military-political threats to complex, multi-domain risks encompassing cyber, informational, climate, biological, and demographic spheres. A defining feature of these challenges is their transnational nature,

which creates an objective need for coordinated international responses while maintaining the leading role of nation-states in ensuring security.

A key obstacle to effective harmonization remains the structural anarchy of the international system, combined with deepening asymmetries between states and increasing geopolitical fragmentation. Strategic competition among leading powers, Russian aggression against Ukraine, and the polarization between authoritarian and democratic regimes have created parallel institutional structures that complicate the search for common solutions to transnational challenges. At the same time, the technological revolution, despite its potential to enhance coordination, generates new sources of instability due to the digital divide and the absence of universal norms of behavior in cyberspace.

The analysis of successful and failed attempts at harmonizing interests has demonstrated higher effectiveness of sectoral integration compared to efforts to create universal governance mechanisms. Networked organizational forms, coalitions of interested states, and the principle of variable geometry prove more adaptive to contemporary challenges. Subnational actors, the private sector, and digital technologies open new opportunities for 'bottom-up' harmonization through the creation of universal standards and practices.

For national governments, it is critically important to develop capacities for differentiated participation in international regimes, create integrated crisis management systems, and foster 'multi-track diplomacy'. The hybrid nature of contemporary threats requires abandoning the traditional separation between domestic and foreign policy, as well as between civilian and military spheres.

Ukraine, positioned at the epicenter of confrontation with authoritarian aggression while simultaneously integrating into European structures, has a unique opportunity to serve as a laboratory for developing new approaches to harmonizing global and national interests. The Ukrainian experience in countering hybrid threats, digitalizing public services, and mobilizing international support can become a model for other countries facing similar challenges. A priority task is the development of strategic communication capable of articulating Ukrainian interests as part of broader global values of democracy, the rule of law, and territorial integrity.

Harmonizing global and national interests in the 21st century requires combining a realistic understanding of the limitations of the existing international system with a readiness for innovation and experimentation in

cooperative formats capable of ensuring an effective response to contemporary transnational challenges.

References

1. On Combating Terrorism: Law of Ukraine dated March 20, 2003, No. 638-IV. Bulletin of the Verkhovna Rada of Ukraine, 2003, No. 25, Art. 180. Available at: <https://zakon.rada.gov.ua/laws/show/638-15#Text>.
2. United Nations Interregional Crime and Justice Research Institute (2024). Report on the Dark Web and Cyber-Crime-as-a-Service and its impact on cyber-enabled terrorism. Turin, 54 p. Available at: <https://www.un.org/counterterrorism/es/node/21245>.
3. Comprehensive Update on Terrorist Financing Risks. Paris : Financial Action Task Force. (2025). 134 p. Available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf>.
4. FATF warns of online terror financing: 'E-commerce and online payment platforms misused' (2025). The Times of India. Available at: <https://timesofindia.indiatimes.com/india/epoms-paypal-and-vpns-pulwama-gorakhnath-cases-cited-as-fatf-warns-of-online-terror-financing-says-e-commerce-and-online-payment-platforms-misused/articleshow/122323762.cms>.
5. The U.S.-Russia New START Agreement: A Fact Sheet. Washington: Arms Control Association (2024). Available at: <https://www.armscontrol.org/factsheets/new-start-glance>.
6. Iran and the IAEA: Monitoring and Verification in the Islamic Republic of Iran in light of United Nations Security Council Resolution 2231 (2015). (2024). Vienna : International Atomic Energy Agency. Available at: <https://www.iaea.org/newscenter/focus/iran>.
7. Nuclear weapons in Belarus: what we know (2024). International Campaign to Abolish Nuclear Weapons. Available at: https://www.icanw.org/nuclear_weapons_in_belarus_what_we_know.
8. European Centre of Excellence for Countering Hybrid Threats (2023). Countering Hybrid Threats: Lessons Learned from Ukraine. Helsinki, 32 p. Available at: <https://www.hybridcoe.fi/publications>.
9. Background to «Assessing Russian Activities and Intentions in Recent US Elections» (2017). Intelligence Community Assessment.

Washington : Office of the Director of National Intelligence. Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

10. World Economic Forum (2025). Global Cybersecurity Outlook 2025. Geneva, 42 p. Available at: <https://www.weforum.org/reports/global-cybersecurity-outlook-2025>.

11. Harper, E., Andrew, J., Foster, F., Niyo, J., Meretti, B., Sturgess, C. (2024). Behind the lens: exploring the problematic intersection of surveillance, cyber targeting and disinformation : research brief. Geneva : The Geneva Academy of International Humanitarian Law and Human Rights, 23 p.

12. Cevik, S. (2022). Climate Change and Energy Security: The Dilemma or Opportunity of the Century? : Working Paper. Washington : International Monetary Fund. 20 p. Available at: <https://www.imf.org/en/Publications/WP/Issues/2022/09/08/Climate-Change-and-Energy-Security-The-Dilemma-or-Opportunity-of-the-Century-523249>.

13. World Health Organization (2023). Climate Change and Health: Key Facts. Geneva. Available at: <https://www.who.int/news-room/fact-sheets/detail/climate-change-and-health>.

14. World Economic Forum, 2025. Global Risks Report 2025. 19th ed. Geneva, 98 p. Available at: <https://www.weforum.org/publications/global-risks-report-2025>.

15. Tuca, S. (2015). Global Governance vs. National Sovereignty in a Globalized World. CES Working Papers. Vol. 7, Iss. 1. P. 193–201.

16. Peterson Institute for International Economics, 2024. Annual Report 2024. Washington, 23 p. Available at: <https://www.piie.com/microsites/2025/annual-report-2024>.

17. Shaping the future of global governance (2024). New York: United Nations University. Available at: <https://unu.edu/cpr/news/shaping-future-global-governance>.

18. ESG Investing: Practices, Progress and Challenges (2020). Paris: OECD Publishing. <https://doi.org/10.1787/5504598c-en>.

Chapter 9
***Formation of a sustainable development model of the state to
ensure national security***
(N. Skorobogatova)

Modern global processes demonstrate the growing interdependence of socio-economic development, environmental sustainability, and national security issues. Sustainable development remains the key concept that provides long-term guidance for global policies. It is defined as a process that meets the needs of the present generation without compromising the well-being of future generations. This process involves striking a balance between three interdependent dimensions: the economic, the social, and the environmental. However, compliance with the principles of sustainable development is insufficient in the face of growing instability. This is why the concept of sustainable development as the ability of systems to function, adapt and recover from shocks is becoming increasingly important.

The relevance of the study is determined by several factors. International policy documents, including the 2030 Agenda for Sustainable Development, the Paris Agreement on Climate Change and the updated strategies of the European Union and NATO, are increasingly incorporating environmental and socio-economic factors into security strategies. Additionally, many states' national strategies are beginning to integrate sustainable development goals into defence and crisis planning, but the methodological basis is not sufficiently developed. Furthermore, modern crises (from the pandemic to energy and food crises) demonstrate that national security cannot be guaranteed without sustainable and resilient development, just as a strong security system is necessary to ensure progress in achieving goals.



The study aims to theoretically identify the relationship between sustainable development, resilience and national security, and to improve the scientific and methodological foundations in order to develop practical recommendations for a sustainable state development model that ensures national security. The study's objectives include analysing the evolution of concepts and their correlation, identifying the main mechanisms of mutual influence, considering the institutional and practical consequences for state policy and developing a model for assessing the sustainable development of the state in the context of national security. The study focuses on forming an integrated approach that combines long-term strategic goals with operational protection and adaptation measures, which are necessary for developing effective national and international policy in the 21st century.

9.1. Theoretical foundations of the sustainable development of society in the context of ensuring national security

Traditionally, sustainable societal development is defined as development that meets the needs of the present without compromising the ability of future generations to meet their own needs [1]. The key principle of this concept is balancing environmental protection, economic growth and social justice [2, 3]. This concept was introduced in the Brundtland Report of 1987 and further consolidated at the Earth Summit in 1992 [4, 5]. Approved by more than 150 countries, the 2030 Agenda for Sustainable Development aims to create a sustainable and resilient world based on achieving the Sustainable Development Goals [6]. The concept of sustainable development is based on addressing economic, environmental, and social issues simultaneously. In particular, it involves integrating economic activity with environmental protection and social issues. This can be achieved by reducing the consumption of material resources, increasing their efficiency of use, enabling their reuse and using sustainable technologies [7]. Key provisions of sustainable development include resource-efficient technologies, structural economic changes towards resource-intensive sectors, and preventive environmental management [8]. No less important are the issues of achieving social justice and cultural diversity. Sustainable development

aims to solve problems such as poverty, inequality and social exclusion. Protecting ecological integrity and reducing environmental impact are also key aspects of sustainable development. This involves the sustainable management of natural resources, reducing pollution, and mitigating the negative effects of climate change. The basic elements of the concept of sustainable development are summarised in Fig. 9.1.

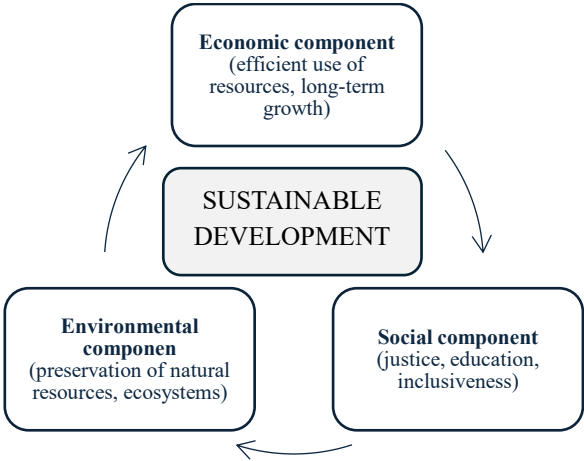


Fig. 9.1. Components of the sustainable development of society

Source: compiled by the author based on [1; 4; 5]

At the same time, the concept of resilient development appears in scientific literature, which causes certain misunderstandings when translating the concepts of sustainable and resilient development into different languages. In the context of accelerating climate change, instability of the global economy, growing geopolitical uncertainty and cyber threats, it becomes evident that the traditional understanding of security, limited exclusively to the military sphere, is insufficient for adequate analysis and development of state development strategies. Scholars note that resilience emphasizes a new way of thinking, taking into account factors of uncertainty and dynamism [9]. The concept of resilience is found in various scientific fields. In particular, Brown K. [10] argues that consideration of the essential features of resilience can fundamentally change the response to global changes, going beyond orthodox approaches to development focused on modernization and economic growth. Pearson L. [11] emphasizes that

resilient systems provide the ability to absorb crises and unforeseen situations while maintaining desired outcomes, unlike traditional equilibrium-based management approaches. Bene C. et al. [12] highlight important limitations, noting that resilience as a concept is not inherently pro-poor and cannot replace poverty reduction efforts, despite its ability to facilitate diverse approaches to addressing social development problems. Thus, the concept of resilience focuses on the ability of social systems to withstand unforeseen or crisis situations, unexpected changes and impacts, while maintaining core functions and structure. The main elements of resilient development are the following:

- adaptability to change, i.e., the ability of a system to modify its own structure, internal processes, and behaviour in response to changing external conditions, while maintaining core functional characteristics;
- post-crisis recovery capacity – the ability to quickly and fully recover after a crisis situation, including the ability to return to the original state or embark on a new development trajectory;
- flexibility of institutional structures, which implies the ability of existing formal and informal rules, norms, and organizational elements to evolve and transform in response to new challenges without complete destruction of the socio-economic system;
- risk diversification, namely the distribution of potential threats and vulnerabilities across different directions, sectors, and sources to reduce overall systemic risk (Fig. 9.2).

A review of scientific sources indicates the existence of a certain interrelationship between the concept of resilience and sustainable development. Three main directions can be identified that characterize their relationship: resilience as a component of sustainability, sustainable development as a component of resilience, as well as resilience and sustainable development as separate but complementary concepts. Both concepts share common goals regarding ensuring benefits for humanity and the environment under normal and extreme conditions. Sustainable development is traditionally defined through environmental, social, and economic considerations, while resilience focuses on the ability of systems to prepare for, absorb, recover from, and adapt to stress or disruptions [13]. Resilience in development relates to the ability to withstand and recover from various challenges, such as climate change and urbanization, while maintaining sustainable growth. Resilience is considered an integral part of sustainable development, focusing on ensuring the future development of

cities and systems. In urban contexts, these two concepts are particularly important for addressing the challenges of rapid urbanization and climate change, as cities implement green infrastructure, resilient design, and community engagement strategies to enhance adaptive capacity while promoting social equity and economic prosperity [14]. Urban resilience involves integrating resilience principles into urban planning to address vulnerabilities and enhance the sustainability of urban areas. Examples of implementing resilience development principles include decentralized water and energy resource management, green infrastructure, etc. Sustainable economic practices, such as integration of renewable energy sources and waste reduction, are crucial for promoting urban resilience. These instruments help balance economic growth with environmental conservation and social justice. Effective governance, community participation, and interdisciplinary collaboration are essential elements for integrating sustainable development and resilience into societal development practices. Essential features of resilient development.

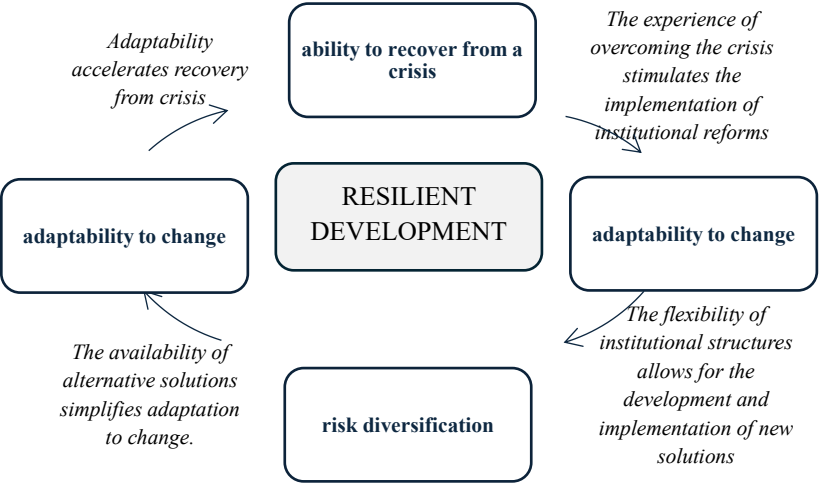


Fig. 9.2. Elements of sustainable development

Source: compiled by author based on [9-12]

Thus, it should be noted that there are an interrelationship and complementarity between the concepts of sustainable and resilient

development. First, sustainable development serves as the foundation for long-term stability of societal development, while resilience ensures the ability of the socio-economic system to maintain the sustainable development trajectory under the influence of external factors. Second, in the temporal dimension, sustainable development is oriented toward ensuring equitable distribution of resources and benefits between generations, toward long-term planning. Meanwhile, resilient development emphasizes the short-term and medium-term adaptive capacity of the system to ensure its long-term existence. Third, a review of scientific research allows us to put forward the thesis about the necessity of ‘sustainable-resilient development’ as a unified paradigm, where sustainable development without resilience becomes vulnerable to crises, and resilient development without sustainability may lead to short-term solutions that can harm the future.

At the same time, fundamental differences between the concepts of sustainable and resilient development should be noted. Sustainable development focuses attention on maintaining balance between the needs of present and future generations. In this context, the economic, social, and environmental dimensions of societal development must be harmonized. Undoubtedly, it is necessary to ensure continuity of development without depleting the resource base and avoiding social conflicts. In contrast, resilient development focuses on the system’s ability to absorb external impacts and adapt to the influence of external factors, while maintaining the functionality of the socio-economic system as a whole and ensuring transformational capabilities when necessary.

Therefore, to ensure societal development in changing conditions while adhering to the principles of sustainable development, it is advisable to apply the tools of adaptive strategic planning based on a scenario approach, which involves developing 3–4 basic development scenarios (optimistic, pessimistic, baseline, transformational) that contain corresponding values of key indicators. Assessment of the actual values of these indicators allows for determining the approximation to one or another development scenario variant. When critical indicator values are reached, pre-developed anti-crisis response measures must be implemented. In order to regularly update the system’s development strategy, it is necessary to conduct monitoring and make possible adjustments every 2–3 years. In addition, a clear system of anti-crisis measures must be developed at all management levels, which will allow not only to respond effectively to crisis situations but also, where possible, to prevent them. This will ensure system resilience while adhering

to the principles of sustainable development. It is also appropriate to introduce adaptive behaviour skills into educational programs in educational institutions, which will allow for the formation of basic knowledge in environmental and financial literacy, develop critical thinking skills when working with information, use practices of implementing interdisciplinary projects, and develop systems thinking.

Thus, the implementation of sustainable and resilient development concepts requires the application of a comprehensive approach at three levels:

- strategic level – changing approaches to planning from periodically developed static plans to adaptive development strategies;
- institutional level – introduction of multi-criteria assessment of resilient and sustainable development into all processes (budgeting, procurement, project evaluation, etc.);
- operational level – development and application of appropriate management mechanisms and instruments (for example, stress tests, early warning systems, diversification programs).

Research into the essence and interrelationship of sustainable and resilient development indicates that achieving long-term goals is impossible without creating mechanisms for adaptation and effective response to crisis situations. Such mechanisms require not only an institutional and resource base, but also the development and implementation of innovative solutions that ensure qualitative changes in the economy, social sphere, and governance. Innovative technologies are becoming one of the drivers of the transition to sustainable and resilient development. In particular, innovations in the field of ‘green technologies’ contribute to reducing environmental burden. Renewable energy, energy-efficient technologies, circular economy, and digital platforms for environmental monitoring allow for ensuring economic growth while meeting environmental requirements. In the social sphere, digitalization of education and digital solutions for providing certain types of social services make society more inclusive and adaptive, which also increases the level of resilience to crisis situations. The application of smart technologies in data processing, public administration, etc., allows for improving the quality of developed forecasts and the effectiveness of crisis response, which is an important argument for preventing crisis situations and overcoming their consequences in the context of ensuring resilient societal development. Thus, without active innovative development, it is problematic to ensure sustainable societal development and make it more resilient and adaptive to the impact of external and internal threats.

In the context of growing uncertainty and external threats, research into issues of ensuring national security is becoming increasingly relevant. National security is a concept that encompasses various spheres of public life and is of critical importance for the functioning and development of states, societies, and individuals. The modern understanding of this concept emerged after World War II, encompassing not only the military aspect but also economic, political, and social dimensions [15]. Modern national security is ensured through the state as the primary security organization, where personal security becomes dependent on national security. Security measures integrate political, diplomatic, economic, military, environmental, social, cultural, moral, and humanitarian spheres to preserve and strengthen the state. National security policies of different countries serve as framework documents that outline the mechanism by which countries ensure the security of all elements of the state, taking into account both internal and external risks while coordinating the activities of various security actors. Thus, national security includes protecting the country from internal and external threats, ensuring the protection of national interests, sovereignty, and fundamental human rights. Effective national security policy requires clear priorities and achievable goals. A review of scientific works indicates the existence of numerous approaches to determining the level of security from different perspectives. A systematization of existing approaches is presented in Table 9.1.

Table 9.1

Components of national security*

Name	Constituent elements	Challenges
Military security: protection from military threats, ability to deter military aggression and defend the country's sovereignty	State defence capability (armed forces, armaments), military strategy, military alliances and partnerships, country's defence-industrial complex, mobilization system	Hybrid wars (combination of military and non-military methods), cyber warfare and information warfare
Political security: stability of the political system, protection of the constitutional order, sovereignty in decision-making	Stability of political institutions, protection from external political influence, effective public administration system	Political conflicts in society, cyber threats, external influence
Economic security: the state of the country's economy that ensures a sufficient level of social, political, and defence existence and development, invulnerability to external and internal threats and challenges	Stability of the national currency, inflation level, resilience of the banking system, level of public debt and international reserves, economic diversification, development of the country's productive and innovative potential, protection from trade wars, export and import diversification, protection of the domestic market	Economic sanctions, financial crises, technological dependence, disruption of supply chains

Table 9.1 (continued)

Energy security: the state of protection of the country and its citizens, the country's economy from threats of deficit in meeting energy resource needs	Diversification of energy sources, diversification of suppliers and supply routes, creation of strategic reserves, development of domestic extraction/production, energy efficiency, reliability of energy infrastructure	Cyberattacks and military attacks on energy infrastructure, climate change, critical dependence on energy resource imports
Food security: the country's population has physical and economic access to sufficient quantities of quality and safe food products at all times	Country's self-sufficiency in basic food products (grain, meat, milk, etc.), creation of strategic food reserves, diversification of import sources, resilience of agricultural development to climate change, food safety and quality	Climate change, land degradation and depletion of water resources, population growth and urbanization, dependence on imports of critical products, military actions
Social security: protection of the social sphere from threats capable of destroying it or substantially changing its qualitative characteristics	Birth-to-death ratio, age and ethnic structure of the population, migration processes, level of social inequality, level of trust in society, absence of acute social conflicts, social protection, healthcare, education, protection of socially vulnerable population groups, preservation of cultural identity	Population aging, wars, mass population migration, social polarization of society, decline in the level and quality of social protection, psychological instability
Environmental security: protection of the environment and vital human interests and needs from possible negative impacts of economic activities, natural and man-made emergencies	Adaptation to climate change, reduction of greenhouse gas emissions, protection from extreme weather events, biodiversity conservation, ecosystem protection, prevention of biological threats, access to drinking water, preservation of soil fertility, forest management, rational use of natural resources, prevention of industrial disasters, waste management	Climate change, biodiversity loss, water, air, and land pollution, drinking water scarcity, land degradation and droughts, transboundary nature of environmental problems
Information security: protection of the national information space, its formation, use and development in the interests of citizens and the state	Protection of critical information infrastructure, countering cyberattacks, personal data protection, financial systems security, countering disinformation, ensuring media literacy of the population, development of domestic technologies	Hybrid threats and information warfare, disinformation, cyber threats to critical infrastructure facilities, interference in electoral processes, artificial intelligence
Technological security: protection of technologies, ability to develop domestic technologies, reduction of dependence on external sources in strategically important sectors	Control over critical technologies, domestic technological developments, protection of intellectual property rights, country's human resource potential, regulatory standards and norms	Technological competition among countries, fragmentation of global technology chains, control over rare natural resources, emigration of highly qualified specialists and working-age population

* Source: compiled by the author based on [14–17]

Generalization of factors influencing the formation of national security allowed for their systematization by direction (positive, negative) and level (external, internal) of impact (Table 9.2).

Table 9.2

National security factors*

Internal factors	
Positive impact	Negative impact
Economic (diversification of the economy, high level of innovative development, developed infrastructure, financial stability, resource-efficient production)	Economic (mono-orientation of the country's economy, for example, a raw material economy, high level of public debt, technological backwardness)
Social (social cohesion of the population, high level of quality of education, developed share of the middle class, low level of socio-economic inequality, stable civil society)	Social (high level of inequality in society, social fragmentation, ethnic and religious conflicts, low level of trust in government)
Political (stability of political institutions, rule of law, effective system of public administration, low level of corruption, use of democratic governance mechanisms)	Political (weak political institutions, corruption, political instability, authoritarianism)
Demographic (favourable demographic structure, high-quality medical care, high proportion of the population with higher education, controlled migration)	Demographic (rapid population aging, depopulation, uncontrolled migration, brain drain)
Geographic (convenient strategic location, access to resources, climatic conditions)	Environmental (environmental destruction, resource depletion, vulnerability to natural disasters)
External factors	
Positive impact	Negative impacts
Geopolitical (stable international environment, friendly relations with partner countries, membership in international organizations, absence of direct military threats)	Geopolitical (regional conflicts, hybrid threats, military conflicts)
Economic (access to global markets, favourable market conditions, attraction of international investments, technology transfer)	Economic (global financial and economic crises, trade wars, economic sanctions, volatility of resource prices, disruption of global chains)
Legal (effective dispute resolution mechanisms, compliance with international norms, protection of national interests through international institutions)	Technological (technological lag, digital addiction, cyber threats)

* Source: compiled by the author based on [14–17]

It is possible to assess the level of security of a country based on international ratings. The Global Peace Index, for example, is a tool developed by the Institute for Economics and Peace that uses 23 quantitative and qualitative indicators to assess three areas: the level of public safety and security, the scale of ongoing internal and international conflicts, and the degree of militarisation. Six statistical indicators are used to assess the duration of internal and international conflicts and determine the degree to which a country is involved in them, including the number and duration of internal conflicts, the number of deaths resulting from internal and external conflicts, the number and duration of external conflicts, the intensity of the conflict and relations with neighbouring countries. The level of public safety and security is determined by analysing the following indicators: perception

of crime in society; number of refugees and internally displaced persons as a percentage of the population; political instability; scale of political terror; impact of terrorism; number of murders per 100,000 people; violent crime rate; violent demonstrations; number of prisoners per 100,000 people; number of internal security and police personnel per 100,000 people; ease of access to small arms and light weapons. The third component of this rating is the level of militarisation, estimated based on the following indicators: military expenditure as a percentage of GDP; number of military personnel per 100,000 people; volume of imports of major conventional weapons per 100,000 people; volume of exports of major conventional weapons per 100,000 people; financial contribution to UN peacekeeping missions; and possession of nuclear and heavy weapons. The ten leading countries by the value of the Global Peace Index in 2025 are presented in Appendix A (Table A.1).

A comparative analysis of the aforementioned 2024-2025 rating data shows that, on average worldwide, the quantitative assessment of 13 out of 23 analysed indicators has worsened. For eight indicators, the assessment has improved, and two have remained unchanged. Thus, we can conclude that the situation has worsened on a global scale.

In this rating, Ukraine ranks 159th out of 163 countries. Its index value is 3,174. The index value varies from 1 to 5; the lower the score, the safer (more peaceful) the country is. Experts identified the following as the biggest threats to our country: access to small arms, the intensity of internal conflict, the number of deaths due to the conflict, the number of refugees and internally displaced persons, and relations with neighbouring countries – all of which received a score of 5 out of 5. This assessment is explained by the war on Ukrainian territory. However, this rating mainly takes into account military security indicators, which does not allow for a full assessment of national security levels.

Another indicator that allows us to assess the level of security in a country to some extent is the Quality of Life Index [19]. This index consists of the following indicators:

- cost of living and purchasing power of the population: Assesses the availability of goods and services in relation to income;
- housing availability: takes into account the cost and availability of housing;
- pollution: measures environmental quality, including air and water quality;

- crime rate: analyses the predicted level of criminal activity and general safety;
- quality of healthcare: effectiveness and accessibility of medical services are taken into account;
- traffic and time spent commuting: examines the average duration and conditions of daily trips.

As can be seen from the list of indicators, this rating focuses more on the socio-economic assessment of the country and how convenient and comfortable it is for the population to live there. The ten leading countries according to this index are presented in Appendix A (Table A.2).

It should be noted that this rating incorporates the Security Index into its calculations. As can be seen in Table A.2, the countries that top the Quality of Life and Security indices differ, due to various factors affecting the formation of each index. For example, Ukraine is ranked 61st out of 88 countries in terms of security (Security Index value 53.0) and 68th in terms of quality of life (Index value 115.0).

To analyse the dynamics of achieving the Sustainable Development Goals, a ranking of countries is compiled according to their degree of achievement of the seventeen Sustainable Development Goals. Fig. 9.3 shows the ten leading countries in this rating and Ukraine. The colour designation allows you to assess the degree to which each goal has been achieved. 167 countries participate in this rating. The Sustainable Development Goals Achievement Index is assessed on a scale from 0 to 100, representing the percentage degree of achievement of the corresponding goal. Therefore, the difference between 100 and a country's SDG Achievement Index score represents the percentage point distance that needs to be covered to reach it. According to data from 2025, Ukraine ranks 42nd. Taking into account the impact of the war on the economy, social and environmental spheres, this is a rather positive result.

As can be seen in Fig. 9.3, all leading countries have a high level of achievement of Goal 1, No Poverty, as these are highly developed countries, but they have problems with Goals 12, Responsible Consumption and Production, and 13, Climate Action. At the same time, this rating also does not allow us to assess the degree of interconnection between sustainable development and national security.

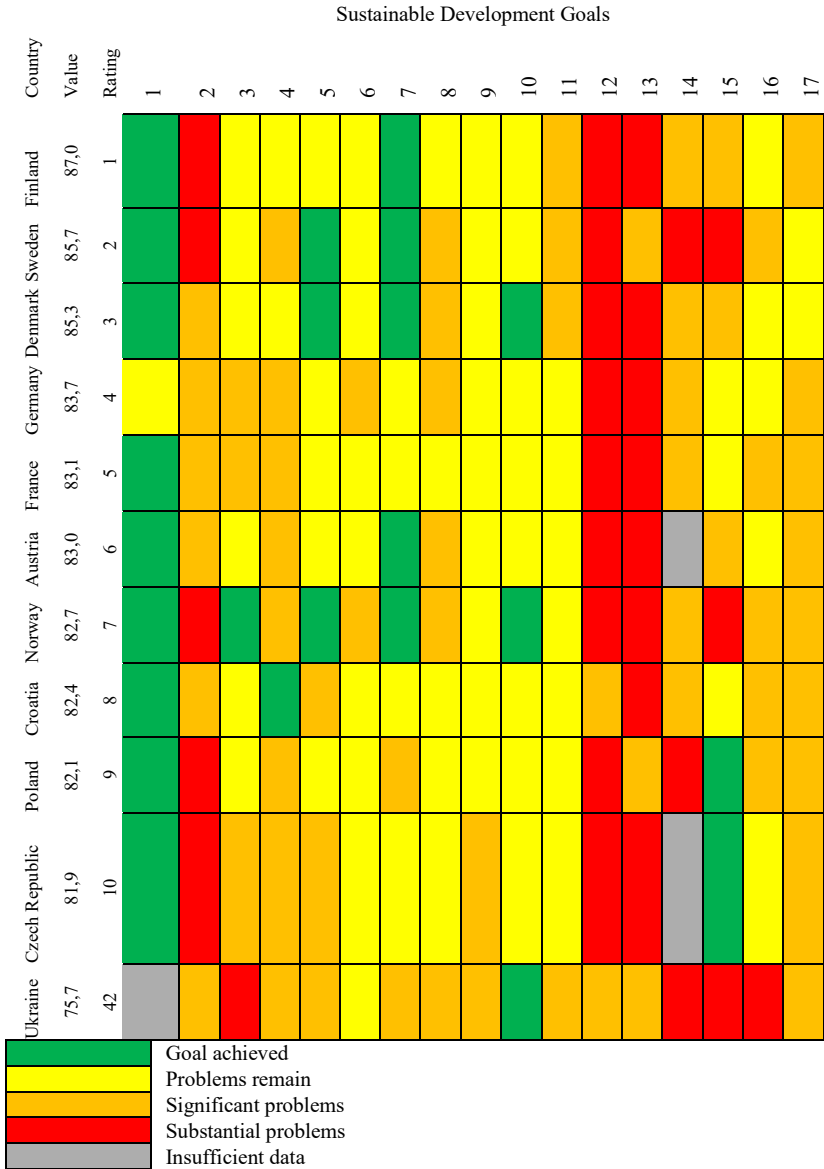


Fig. 9.3. Leading countries according to the GSD Index and Ukraine, 2025

** Source: compiled by the author based on [20]*

Thus, it can be noted that the concepts of sustainable development and stability are increasingly being used in assessing a country's development. Adherence to the concept of sustainable development in formulating a state development strategy allows long-term goals and objectives to be set, while adherence to stability makes it possible to achieve these goals in conditions of risk and uncertainty. In this context, it is appropriate to consider sustainable development as a state that society strives to achieve, and sustainable development as a condition or opportunity to achieve this result. At the same time, the concepts of sustainable and stable exist at different levels of management – at the level of the ecosystem, the national economy, infrastructure elements, state institutions, business units, etc. Using a systematic approach, it should be noted that sustainable development determines the long-term development trajectory at the relevant level of governance (long-term goals, objectives, key indicators), while the resilience of development determines the level of readiness to achieve the set goals in both the medium and short term, taking into account the impact of crises and emergencies. Therefore, the development of a state development strategy should be based on a sustainable development programme (investment programmes, legal frameworks, etc.) that includes elements to increase the resilience of the system (use of adaptive mechanisms, rapid response mechanisms, protection of critical infrastructure or the ability to duplicate certain functions). A similar approach should be used at the meso- and micro-levels. Ignoring the principles of sustainable development and system stability can negatively affect national security. For example, lack of progress in achieving sustainable development goals related to poverty eradication (SDG 1), ending hunger (SDG 2), and reducing inequality (SDG 10) creates vulnerabilities in the system that can lead to internal social unrest and exacerbate geopolitical conflicts. Therefore, the national security strategy should include measures to achieve sustainable development as a contribution to long-term stability in society.

Despite the identified interconnection between the concepts of sustainable development and national security, it should be noted that certain conflicts may arise in the definition and implementation of objectives. For example, the mobilisation of resources for the immediate defence of the country against military aggression may negatively affect the financing of long-term environmental development programmes. Similarly, strategic 'green industry' projects may cause territorial disputes or temporarily exacerbate economic inequality between territories. Therefore, the

management task is to find compromise solutions and institutional mechanisms that would allow for the simultaneous maintenance of operational security and long-term sustainability.

Thus, we believe that, given the deep interconnection between the concepts under consideration, the state development strategy should focus on several key areas, namely:

- integrating sustainable development goals into national security strategies;
- investing in infrastructure and environmental sustainability (energy independence, food security, etc.);
- developing human capital and social protection systems;
- creating mechanisms for interagency cooperation and risk assessment (e.g., including climate risk and cyber threats);
- deepening international cooperation, including both financial and technical areas, which will contribute to the joint resolution of similar issues.

9.2. Model of sustainable development of the state to ensure national security

When examining the essence of sustainable development, it was noted that it is based on three pillars, namely: environmental, social and economic. The environmental component is determined by tools for solving environmental problems, rational use of natural resources, and the possibility of their replacement and restoration. Such tools include encouraging the transition to renewable energy sources and green technologies, introducing a circular economy, proper urban planning, etc.

The social component combines public policy, various initiatives, etc., aimed at solving social problems in society. For example, within the social context, states must combat poverty, ensure a decent quality of life for the population, and provide equal access to education and healthcare.

The economic component emphasises the importance of business viability and sustainability. In order for a business to be both sustainable and profitable, tax instruments are used, for example, to impose tax penalties for environmental pollution and to provide incentives for conscientious companies, as well as quotas and licensing of activities, etc.

At the same time, on the path to sustainable development, governments face challenges such as instability, inequality, lack of effective leadership, lack of necessary investment, economic disparities between urban and rural

development, conflicts within and between states, further depletion of natural resources and climate change, etc. In such conditions, the issue of ensuring national security and developing forecasts for sustainable development becomes particularly relevant. Current approaches to measuring sustainable development in countries do not take into account the state of national security and security in general.

An analysis of literary sources has led to the conclusion that existing scientific approaches define sustainable development of a state on the basis of three main components: economic, environmental and social. However, we consider it appropriate to expand the classical triad and add a fourth component – innovation and security. This addition is justified and necessary in view of the current realities of global development. In the context of the high degree of uncertainty that characterises the modern world order, the existence of various threats to the sovereignty of states and the security of citizens, global instability and geopolitical challenges, the issue of ensuring national security is of paramount importance. Without guaranteeing the security of the state and its citizens, it is impossible to ensure the effective implementation of any of the three traditional components of sustainable development. This is especially relevant now for our country, which is at war. Military actions pose a serious and immediate threat to the implementation of sustainable development goals not only in Ukraine, but also in many other countries around the world. War is a major obstacle to ensuring food, economic, social and environmental security at the national, regional and global levels. War destroys economic infrastructure, spreads environmental disasters, creates humanitarian crises and destabilises food security on a global scale. At the same time, war stimulates innovation in the fields of defence, medicine, energy and digital technologies. The innovation and security component is an essential element of the country's national development strategy.

The modern world is characterised by rapid technological change and innovative transformations. The fourth industrial revolution, digitalisation, artificial intelligence, biotechnology and other innovative technologies are radically changing economic, social and environmental processes in society. Without the active introduction of innovations, the state will not be able to ensure the competitiveness of the national economy, effectively solve environmental problems and meet the social needs of society. The innovative component is becoming an important factor in determining the possibility of achieving other components of sustainable development. Currently, in

conditions of high global uncertainty and the existence of various threats to the sovereignty of states and the security of citizens, the issue of ensuring national security is becoming critical. Cyberattacks, hybrid wars, terrorist threats, pandemics, energy dependence, climate change, and military conflicts create new challenges that were not relevant when the classic concept of sustainable development was formulated. Without guaranteeing the security of the state and its citizens, it is impossible to ensure stability and predictability of development in any of the traditional spheres.

Furthermore, innovation and security are closely intertwined. On the one hand, innovative technologies are critical to national security, as cybersecurity, military technologies, and energy independence are based on innovation. On the other hand, a secure environment is a prerequisite for innovation, as research, development, and implementation of new technologies require stability, intellectual property protection, and long-term investment. The experience of leading countries shows that investment in innovation and security are factors that reinforce economic growth. Countries that are leaders in sustainable development indices are also leaders in innovative development and have a high level of national security.

The following countries were selected for comprehensive research: Belgium, Bulgaria, Italy, China, Lithuania, Germany, Poland, Romania, Ukraine, and the Czech Republic. The selection of these countries is justified and methodologically sound, as Ukraine will be able to borrow the experience of foreign partners to achieve sustainable development goals in its own conditions. The different preconditions for development in these countries, the measures they have taken and the results they have achieved will enable our country to create an optimal and adapted strategy for achieving sustainable development. An analysis of the experience of countries with different levels of economic development, geographical location and historical characteristics will reveal universal principles and specific mechanisms for ensuring sustainable development that can be adapted to Ukrainian realities, taking into account current challenges and threats to national security.

The analysis of the components of sustainable development in countries was carried out in accordance with the following four components (Fig. 9.4).

The structure of the sustainable development index is based on an integrated approach that combines the three classic components (economic, environmental, social) with the proposed innovation and security component. The choice of indicators for calculating the integral index is justified by the

logical interconnection of indicators and the availability of open data for calculations. It is proposed to assess the economic component using the following indicators: GDP per capita, inflow of foreign direct investment, and outflow of foreign direct investment.

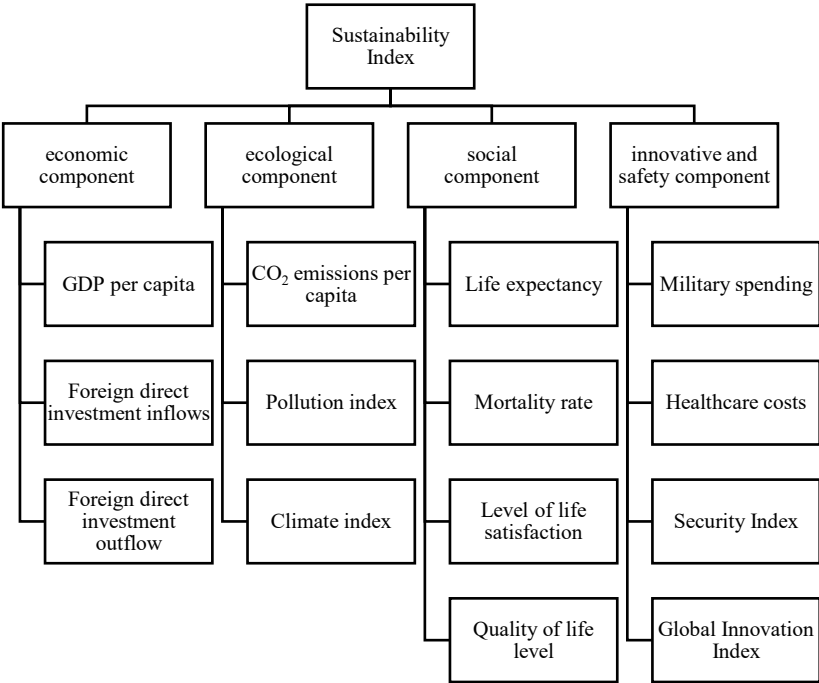


Fig. 9.4. Structure of the index of sustainable development of the state in the context of ensuring national security

** Source: compiled by the author based on [17]*

GDP per capita – this indicator is one of the main indicators of economic well-being and productivity of a country's economy. It reflects the average level of production per person and characterises the state's potential to meet the needs of the population. The developed model proposes to include not the total GDP, but GDP per capita, since the latter indicator allows comparing the economic power of different countries, taking into account their size and population.

Foreign direct investment inflows – foreign direct investment (FDI) demonstrates the degree of confidence of international investors in the country's economy and its investment climate.

Outflow of foreign direct investment – this indicator characterises the ability of national economic entities to invest abroad. A balanced ratio of investment inflows and outflows is a sign of a developed economy.

The environmental component is proposed to be determined based on the following indicators: CO₂ emissions per capita, pollution index, climate index.

CO₂ emissions per capita are proposed to be included in the model, since the carbon footprint is one of the prominent indicators of the country's impact on global climate change. This indicator indirectly takes into account the efficiency of energy resources use, the level of development of the “green” economy. This indicator is directly related to the Paris Climate Agreement and the UN Sustainable Development Goals.

The pollution index is a complex indicator that reflects the overall level of environmental pollution, including air, water and soil pollution.

Climate index – this indicator assesses the degree of vulnerability of the country to climate change, the effectiveness of the measures taken and the effectiveness of the implementation of climate policy in the state. The climate index reflects the readiness of the state to the challenges of global warming and other changes.

The social component is proposed to be assessed by the following indicators: life expectancy, mortality rate, level of life satisfaction, level of quality of life.

Life expectancy is an integral indicator that reflects the effectiveness of the health care system, social protection, level of nutrition, sanitary conditions and general well-being of society.

The mortality rate of the population indirectly characterizes the availability and quality of medical services, social security of the population.

The level of life satisfaction reflects the psychological and socio-economic state of the population, the quality of social institutions and the general standard of living.

The level of quality of life is a comprehensive indicator that also integrates various aspects of life: access to education, medical services, housing, cultural goods, environmental quality, security and social infrastructure.

The innovation and security component is proposed to be determined on the basis of healthcare spending, military spending, the security index and the global innovation index.

Military spending – this indicator characterizes the ability of the state to ensure its own security and sovereignty in conditions of geopolitical instability. Military spending allows us to take into account national security priorities, the level of threats and the country's readiness to defend national interests.

Healthcare spending is an investment in healthcare, which can be considered one of the main elements of human capital development. This indicator reflects the ability of the healthcare system to counteract epidemics, pandemics and other threats to public health.

The Security Index is a comprehensive indicator that assesses the degree of personal security of citizens, the level of crime, the effectiveness of law enforcement agencies, the judicial system and the general level of law and order.

The Global Innovation Index – this indicator assesses the innovative potential and effectiveness of the country's innovative activity. It includes such parameters as investment in science and education, patent activity, the development of high-tech production, the degree of digitalization of the economy and the development of innovative infrastructure. The Global Innovation Index is a critical indicator of the competitiveness of the economy in the conditions of the fourth industrial revolution and determines the country's ability to adapt to technological changes.

The information base for building a model for assessing the sustainable development of the state in the context of ensuring national security was open databases, presented in Table 9.3.

Thus, it is proposed to determine the level of sustainable development of the state to ensure national security as follows:

$$ISD = k_1 Ec + k_2 En + k_3 S + k_4 IS, \quad (1)$$

where ISD – the index of sustainable development of the state in the context of ensuring national security;

k_1, k_2, k_3, k_4 – weighting factors to take into account the degree of significance of the economic, environmental, social and innovation-security components, respectively;

Ec, En, S, IS – economic, environmental, social and innovation-security components of sustainable development of the state.

$$ISD = k_1 \sum_{i=1}^3 Ec_i + k_2 \sum_{j=1}^3 En_j + k_3 \sum_{h=1}^4 S_h + k_4 \sum_{g=1}^4 IS_g \rightarrow \max \quad (2)$$

Table 9.3

Indicators of the model for assessing the sustainable development of the state

Indicators		Source	
		Resource name	Link to data source
Economic component			
x1	GDP per capita	The World Bank. GDP per capita (current US\$).	https://data.worldbank.org/
x2	FDI inflow	UNCTAD. Global foreign direct investment flows over the last 30 years.	https://unctad.org/data-visualization/global-foreign-direct-investment-flows-over-last-30-years
x3	FDI outflow		
Environmental component			
x4	CO2 emissions per capita	Our World in Data. CO2 emissions.	https://ourworldindata.org/co2-emissions
x5	Pollution index	Pollution Index	https://www.numbeo.com/
x6	Climate index	Climate Index	
Social component			
x7	Life expectancy	The World Bank. Life expectancy at birth, total (years)	https://data.worldbank.org/
x8	Mortality	The World Bank. Death rate, crude (per 1,000 people)	https://data.worldbank.org/
x9	Level of life satisfaction	Our World in Data. Self-reported life satisfaction.	https://ourworldindata.org/happiness-and-life-satisfaction
x10	Quality of life	Quality of Life Index	https://www.numbeo.com/
Innovative and safety component			
x11	Military spending	The World Bank. Military expenditure (% of GDP)	https://data.worldbank.org/
x12	Healthcare costs	The World Bank. Current health expenditure (% of GDP)	https://data.worldbank.org/
x13	Security Index	Safety Index	https://www.numbeo.com/
x14	Global Innovation Index	Global Innovation Index	https://www.wipo.int/

The values of indicators that negatively affect the achievement of sustainable development of the state (CO₂ emissions per capita, pollution index, mortality) are taken as negative (with a ‘-’ sign), and indicators whose values positively affect the implementation of sustainable development goals are taken as positive (with a ‘+’ sign). Since the indicators taken into account in the proposed model have different units of measurement, they must be normalized and accepted for further calculations. Accordingly, by analysing

the dynamics of the sustainable development index for a particular country, one can draw a conclusion about the trends in ensuring its development in this direction. Similarly, by comparing several countries by the sustainable development index, one can assess which of the countries has achieved greater success in adhering to the concept of sustainable development, taking into account the security context.

For the analysis, data for the period 2012–2020 were selected, taking into account the availability and openness of information. Using the proposed approach, sustainable development indices were calculated for the analysed countries (Fig. 9.5).

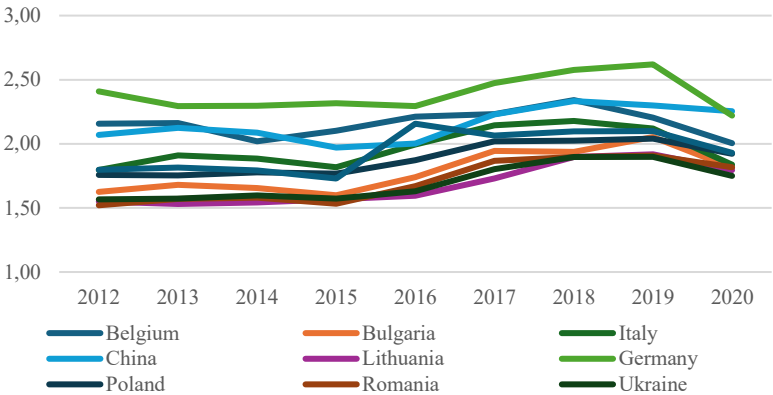


Fig. 9.5. Sustainable development indices for selected countries to ensure national security

The most stable country, based on the calculated values of the sustainable development indices, is Germany, since this country demonstrates better results compared to the analysed countries when calculating the environmental, economic and social components. In particular, this country has good results in terms of investment movement indicators, healthcare spending, life satisfaction, etc. The dynamics of changes in indicators for each country is unstable, among the main trends it can be noted that a positive trend is observed for all countries (the trend line has a positive slope), and in 2020 a decrease in the sustainable development indicator is observed, which is closely related to the beginning of the COVID-19 pandemic. Unfortunately, the last places in the ranking are occupied by Ukraine and Bulgaria, whose sustainable development indices differ little

from each other. Of course, the calculations took into account indicators by country until the beginning of 2022, which reflects the state of development of the countries before the start of military operations in Ukraine. Therefore, sustainable development in modern conditions is an integral component of national security of states, which requires a comprehensive approach with the integration of innovative technologies and strategic planning. The introduction of a system of national indicators of sustainable development, integrated into strategic planning documents, will ensure coordination between economic, environmental and social policies, creating a synergistic effect to strengthen national security through the prism of long-term sustainability.

Appendix A

Table A.1
Leading countries in the Global Peace Index, 2025*

Country rating	Country	Index value
1	Iceland	1.095
2	Ireland	1.26
3	New Zealand	1.282
4	Austria	1.294
5	Switzerland	1.294
6	Singapore	1.357
7	Portugal	1.371
8	Denmark	1.393
9	Slovenia	1.409
10	Finland	1.42

** Source: compiled by the author based [18]*

Table A.2

Leading countries in terms of Quality-of-Life Index and Safety Index, 2025*

Quality of Life Index			Security index		
Country rating	Country	Index value	Country rating	Country	Index value
1	Luxembourg	220.1	1	United Arab Emirates	84.5
2	Netherlands	211.3	2	Qatar	84.2
3	Denmark	209.9	3	Taiwan	82.9
4	Oman	208.9	4	Oman	81.7
5	Switzerland	205.0	5	Hong Kong (China)	78.5
6	Finland	203.8	6	Armenia	77.9
7	Iceland	202.0	7	Singapore	77.4
8	Norway	195.0	8	Japan	77.1
9	Qatar	193.3	9	Estonia	76.3
10	Sweden	193.2	10	Slovenia	76.2

* Source: compiled by author based on [19]

References

1. Five Principles of Sustainable Development. Sustainable Development Commission. Available at: <https://www.sd-commission.org.uk/>
2. Cortés, M. E. T., Espino, X. M., García, M. J. (2025). Production of Silver Jewellery in Taxco, Guerrero, Mexico, Versus the Objectives of Sustainable Development. *Mining Impacts and Their Environmental Problems*, pp. 197–207. https://doi.org/10.1007/978-3-031-72127-4_11
3. Skorobogatova, N. (2022). Formation of sustainable development of competitive business in an unstable economy. In: IEEE 3rd International Conference on System Analysis & Intelligent Computing (SAIC). Kyiv, Ukraine. <https://doi.org/10.1109/SAIC57818.2022.9922912>
4. United Nations. (1987). Report of the World Commission on Environment and Development: Our Common Future [Electronic resource]. Available at: <https://sustainabledevelopment.un.org/content/documents/5987ourcommon-future.pdf>

5. Skorobogatova, N. (2019). Sustainable development of an enterprise under industry 4.0 conditions. *International conference on creative business for smart and sustainable growth* (CREBUS). IEEE, 2019, pp. 1–5. <https://doi.org/10.1109/CREBUS.2019.8840049>
6. Transforming our world: the 2030 Agenda for Sustainable Development. UN. *Department of Economic and Social Affairs*. Available at: <https://sdgs.un.org/2030agenda>
7. Perdan, S. (2010). The Concept of Sustainable Development and its Practical Implications. *Sustainable Development in Practice: Case Studies for Engineers and Scientists*, pp. 3–25. <https://doi.org/10.1002/9780470972847.ch1>
8. Skorobogatova, N. (2025). Resource Provision for Crisis Management Measures in Local Communities: Accounting and Investment Aspects. Bulletin of the Academy of Labor, Social Relations and Tourism. Series: Economics, Psychology and Management, 5. <https://doi.org/10.54929/3041-2390-2025-05-01-03>
9. Galantini, Z. D. Y., Tezer, A. (2018). Review: In the complex epoch is sustainability “out” resilience “in”? *Environmental Science, Philosophy, Economics*. Available at: <https://api.semanticscholar.org/CorpusID:135363694>
10. Brown, K. (2015). Resilience, Development and Global Change. London. Routledge. 228 p. <https://doi.org/10.4324/9780203498095>
11. Pearson, L. (2008). Applying 'resilience thinking' for sustainable development. *Environmental Science, Economics*. <https://doi.org/10.1071/EC142P16>
12. Béné, C., Newsham, A., Davies, M., Ulrichs, M., Godfrey-Wood, R. (2014). Review article: resilience, poverty and development. *Journal of International Development*. Volume 26, Issue 5 pp. 598–623 <https://doi.org/10.1002/jid.2992>
13. Marchese, D., Reynolds, E., Bates, M., Morgan, H., Clark, S., Linkov, I. (2018). Resilience and sustainability: Similarities and differences in environmental management applications. *Science of the total environment*. Volumes 613–614, pp. 1275–1283. <https://doi.org/10.1016/j.scitotenv.2017.09.086>
14. Singh, A. (2024). Urban Resilience and Sustainability: A Comprehensive Review. *Journal of Sustainable Solutions*. 15(2), 33–38. <https://doi.org/10.36676/j.sust.sol.v1.i2.12>

15. Khan, E. M. (2022). Comprehensive national security: contemporary discourse. *Margalla Papers*, 26 (I): 1–17. <https://doi.org/10.54690/margallapapers.26.I.94>.

16. Skorobogatova, N. (2023). The Influence of innovations on the formation of the economic component of national security. *Створення, охорона, захист і комерціалізація об'єктів права інтелектуальної власності: матеріали VI Всеукраїнської науково-практичної конференції з міжнародною участю, (26.04.2023, м. Київ):* ел. збірник / Упоряд.: В. В. Дмитренко, Ю. М. Перга. Київ: КПІ ім. Ігоря Сікорського, 2023, с.298–303. Available at: <http://cpdcipr.kpi.ua/article/view/278823/273479>

17. Дорошенко, О. С., Скоробогатова, Н. Є. (2023). Чинники збалансованого розвитку країн в умовах мінливого безпекового середовища. Науковий вісник Національної академії статистики, обліку та аудиту: зб. наук. праць. № 3–4. С. 86–96.

18. Global Peace Index. (2025). Institute for Economics & Peace. Available at: <https://www.visionofhumanity.org/maps/#/>

19. Quality of Life Index by Country. (2025). Numbeo. Available at: <https://www.numbeo.com/quality-of-life>

20. SDG Index. (2025). SDG Transformation Center. Available at: <https://sdgtransformationcenter.org/>

Chapter 10
***Coordinating security actions in Europe based on common
perceptions of economic competition and logistics***
(S. Kuzminov)



The global security system is multidimensional and encompasses economic security, which necessitates a sufficient level of competition in transportation and logistics.

This chapter explores models of spatial support for competition in the global security system.

10.1. Actuality, methodology and object of study

Methodology. The research primarily takes an institutional approach, emphasising a unique methodology. Institutions are understood as societal norms that guide the evaluation of various objects, events, and conditions as either positive or negative, desirable or undesirable, and acceptable or unacceptable. These institutions exist within the human mind and lack formal expression. This distinguishes them from organisational forms (organisations), which, particularly in modern contexts, possess formal documentation – such as founding documents, laws, codes, or agreements – that evidences their existence.

Since institutions are informal, they cannot be studied directly through strict scientific methods. Instead, institutions manifest indirectly through their effects, such as value-based decisions made in real life. The complex influence of institutions requires a combination of methods to study the traces of their existence. Our study utilises a historiographic method as its foundation while also incorporating elements of mathematical modelling, content analysis, and graphical abstractions.

To pre-empt potential criticism, let us note that the formation of institutions in human consciousness renders them not only dependent but also woven from human biases, heuristics, beliefs, and other elements that contradict the principles of rational thinking. Therefore, unfortunately, the logically sound scientific research method based on potentially falsifiable

hypotheses and their subsequent testing, known as falsificationism, would simply exclude institutions from consideration. In other words, we would lose the object of our study. Conversely, verificationism, which is inherently unreliable from a strictly evidentiary perspective and is based on assumptions that can be adequately supported by corroborative evidence, keeps institutions within the field of view. Hence, fully aware of the chosen method's limitations, we employ it in our study.

Object of Study. The study focuses on models of spatial provision of competition. The knowledge base of modern economics forms a multi-layered structure of various models. Upper-layer models are used to shape business strategies and legislation, and are relatively commercializable. At the same time, more fundamental models draw far less attention, which carries potential risks. Often, when addressing current challenges, we encounter limitations stemming from our fundamental understanding (or lack thereof) of economics, politics, and society.

With a chessboard, we can play different games of chess, analyse openings, middle games, and endgames, as well as solve chess puzzles. On a chessboard, we can even attempt to play checkers (although the chessboard is not suitable for all versions of this game). However, on a chessboard, it is impossible to play, say, billiards or hundreds of other board games. In fact, the thought wouldn't even occur to us. The situation is the same with fundamental models. Economists have used fundamental models of man, time, space, and competition for decades and even centuries without noticing it. Politicians, lawyers, and other users of economic knowledge often encounter practical problems, but they cannot obtain adequate advice from fundamental science, even without realising why.

One of such fundamental but inconspicuous models is the model of spatial provision of competition. This model defines a worldview but remains in the background, setting boundaries for many decisions in economics and politics. This model remains outside the purview of researchers for several reasons:

1. The spatial provision of the competition model is a component of models of seller behaviour in the goods market (perfect competition, monopolistic competition, oligopoly, and monopoly). In turn, seller behaviour models implicitly form the basis for the Marshallian model of market pricing. Ultimately, the market pricing model establishes the boundaries of what is acceptable and unacceptable concerning the distribution of economic resources to meet needs. Thus, the spatial provision

of the competition module is a 'third-level basement' even within the general theoretical model of market resource allocation. Not to mention its role in competition legislation, economic policy development, and current commercial projects. Under such conditions, few think of delving into such depths.

2. Models of spatial provision of competition are geographically and historically determined. Naturally, they allow some flexibility even within a given region, albeit with certain caveats. However, economic entities do not make a truly conscious choice in favour of one model or another. Furthermore, implementing a model generally depends on a large number of decision-makers. These individuals often have different, sometimes opposing interests, and thus do not pursue a genuinely coordinated policy regarding the logistical support of competitive opposition. Nevertheless, they make decisions based on certain value-based assumptions that are instilled in us from childhood, both in daily life and in education. It is simpler to adopt the values of the community you belong to than to seek something else, likely distant in space and time.

Under such conditions, it is not surprising that the question of analysing models of spatial provision of competition is not only unresolved but also unasked. One might think it is unimportant because it is too theoretical. However, this is not the case. The unresolved nature of this question leads to an inability to answer other, clearly pressing issues. For example, questions about whether the prospects for post-war reconstruction in Ukraine will improve if the Ukrainian army succeeds in liberating territory within the 1991 borders. Or questions about whether the territory of the Russian Federation should be left as it is to ensure Europe's energy security, as some European politicians, not only pro-Kremlin ones, sometimes suggest. The 'hanging' of these questions makes it impossible to form a strategy for the Ukrainian state's goals in the war, which, in turn, leads to misunderstandings of Ukrainian messages by its allies.

Variations of the Spatial Provision of Competition Model in Europe.
The general form of the model for ensuring an adequate level of competition in the market can be presented as a set of three conditions:

$$\begin{cases} \sum_{i=0}^n S_i = 1 \\ S_i \leq S_{max} \\ i \geq N_{max} \end{cases}$$

The first condition specifies that we form a complete set of subjects, taking into account all operators in the market. The total of their market shares, S_i , equals 1 (or 100%). According to the second condition, no single market participant should hold an excessively large market share. The third condition states that the number of these shares should not be too small.

Each of these conditions appears logical, but attempts to apply them in practice reveal many subtleties. For instance, there is a problem of defining S_{max} and N_{max} .

Common sense suggests that the focus is not on the numbers per se, but rather on ensuring the effective functioning of markets. However, “common sense” varies from person to person, especially in disputes. Therefore, in practice, the right to define the maximum safe parameters for market share distribution is delegated to an arbitration or antitrust authority, the name and powers of which vary by country. Some countries set clear numerical parameters, while others do not, essentially relying on arbitrarily chosen criteria and covering the lack of theoretical justification with the authority of state power.

Another issue is defining market boundaries. In essence, modern antitrust practices are still closely tied to the idea declared during the Peace of Augsburg: *Cuius regio, eius religio* (‘Whose realm, his religion’). Market boundaries are defined by the jurisdiction of government bodies, which operate within political borders. However, the growth of international trade undermines the viability of this approach. In the context of globalisation, the operational space of major market players extends far beyond national borders, while international cooperation on antitrust legislation is persistently hampered by the states’ desire to protect their national interests. Nonetheless, this process is gradually advancing thanks to the efforts of international trade organisations.

The question of spatial provision of competition remains a gap in this field. It is essential to differentiate it from models of spatial product differentiation in monopolistic competition, such as ‘City on a Line’ or ‘City on a Circle’ (for more details on spatial competition models, see Biscaia R., Mota I., 2013). A key feature of the models used to analyse spatial competition is the implicit assumption that a product appears out of nowhere, simply at the points of sale. The model itself focuses only on differences in the behaviour of market entities due to geographic distribution within the market. However, in modelling the spatial provision of competition, the focus shifts beyond the market, and the analysis considers the geographical features

of the macroregion. In other words, the spatial provision of the competition model focuses not on what happens within the market but on what occurs beyond its boundaries.

Since our study is Eurocentric, we propose to limit the analysis to two models and one variation of the spatial provision of competition:

1. The Web-Model.
2. The Net-Model.
- 2a. The Transport Corridor Model.

This rather brief list of potential models is determined, firstly, by objective geographical constraints (for communications, there are seas, coasts, and land with varying degrees of transport convenience) and, secondly, by the institutionalisation of relationships within the system of spatial provision of competition. Following T. Veblen, we define institutionalisation as a societal habit, clarifying that institutions are the result of a society's prior developmental trajectory. They establish the prevailing notions of good and bad, desirable and undesirable, acceptable and unacceptable. When establishing a logistical system in international trade, each individual subject operates in a mode of uncertainty and risk and has no choice but to proceed by trial and error, relying on heuristics. When a heuristic proves successful in route finding, positive experience is reinforced. Entities with negative experiences simply disappear from the system, having gone bankrupt. Thanks to this, natural selection is quite intense, and the system quickly transitions from a trial phase to an institutional phase, where revisions to previously established evaluative patterns occur extremely rarely or, in many cases, never.

10.2. Web-Model

The Web-Model is spatially associated with coastal cities that also serve as trade centres (Fig.10.1). Such a city, in its classic form, is centred around a marketplace and/or port, has an umland (the surrounding area it serves), and an extensive system of sea trade routes. The concept of such a city has existed in Europe since at least the time of ancient Athens and remains popular to this day. This format is relevant for cities like Amsterdam, London, and Edinburgh, as well as the merchant republics of Venice and Genoa, the Hanseatic cities of Lübeck, Gdańsk, Copenhagen, and many other similar coastal cities – dozens, if not hundreds, of which still exist.

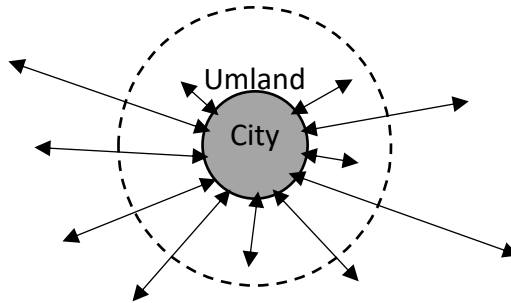


Fig. 10.1. Graphical Representation of the Web-Model

Of course, real sea routes to and from a seaport only loosely resemble a symmetrical web. However, perfect symmetry is not what's important here. The main idea lies elsewhere: routes for delivering goods to the market may differ in geographic distance, but the cost of delivery does not vary so significantly due to the efficiency of maritime transport. Furthermore, blocking transportation in open waters, even with modern naval technology, presents a significant challenge. Throughout history, blockades have been possible only at certain key points – near port areas or in narrow straits. Moreover, blockades have always been, and remain, extremely costly, risky, and generally short-lived measures. Given these characteristics, a geographically asymmetrical system of routes appears much more symmetrical if we consider it from the perspective of the feasibility and cost of delivering goods by sea. Therefore, in the Web-Model, the market can be viewed as spatially open for the delivery of goods (by sea) with a single central point controlling the flow (the port).

Until the end of the 19th century, when ships with steel hulls were introduced, the carrying capacity of wooden vessels was modest, even in comparison to the rather limited market volumes of the time. Accordingly, delivery shipments were small in size but frequent. Additionally, for centuries (until the invention of radio at the end of the 19th century), each ship captain maintained a certain degree of commercial independence. This independence may not have been particularly pleasing to the owners of large trading companies who owned these ships. However, it was practically unavoidable, simply because any central office (if it existed) could not predict prices in overseas markets in advance, nor could it obtain information and conduct

negotiations with the captain or buyers in real-time. Thus, the captain remained an independent merchant.

Thus, we have the following points:

- numerous traders with relatively small shipments of goods can easily enter the market or, if trading here becomes unprofitable, exit it;
- they do not form coalitions and cannot exploit the market situation to their advantage for long, simply due to their size and the brief duration of their ships' stay in port;
- the only source of distortion in an otherwise ideal market mechanism is the state, which collects port taxes and sometimes discriminates against traders at the prompting of local lobbyists.

This is nothing but a set of characteristics of a perfectly competitive market from a microeconomics textbook. At the same time, it is a pattern set for forming a *market institution* – that is, a generalised societal notion of an ideal model of market self-regulation to strive for. And since institutions are significantly more stable and durable than the real organisational forms of market interactions, the perfectly competitive market remains an elusive but still highly desirable ideal for economic regulators.

The problem, however, is that the notion of spatial provision of competition based on the Web-Model persists not only in the unrealistic models of perfect competition found in textbooks but also in actual political decisions. For example, there is the desire to force Putin to pay an unacceptably high price for his aggression against Ukraine to stop him. This is entirely logical and would work within the Web-Model (if Putin shared this perspective), but it carries very little weight within the framework of the Net Model, which, judging by the strategic decisions of Moscow, defines the evaluative patterns in the Kremlin.

10.3. Net-Model

The Net-Model, in contrast, is better suited for describing the realities of spatial provision of competition on land. While at sea, there are only a handful of narrow points where transit traffic can be controlled (such as Turkey's Bosphorus and Dardanelles, Denmark's Oresund Strait, and the more recently constructed Suez and Panama Canals), on land, almost everything consists of narrow points. Forests, swamps, steep slopes, bodies of water, or areas lacking potable water – all serve as obstacles to quick and efficient movement. As a result, despite people's potential ability to move in

any direction on land, a network of intersecting routes forms in reality. The Net-Model can be schematically represented as follows (Fig.10.2).

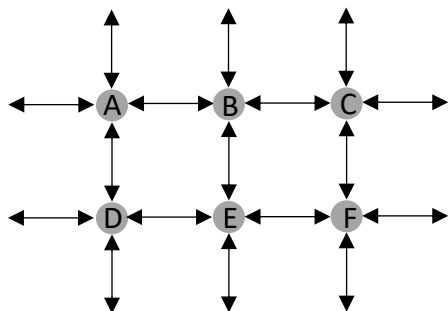


Fig. 10.2. Graphical Representation of the Net -model

Unlike sea routes, land transportation is highly dependent on distance and terrain. The costs on land per unit of cargo moved are many times higher than at sea. At sea, differences in distance can be negligible (within certain permissible limits), but on land, every kilometre and every turn counts.

This creates prerequisites for transforming space into a resource. In our research, we interpret the term ‘resource’ in the broadest sense possible. A resource is any component of the economic process, the removal of which would decrease the efficiency of this process or even halt it entirely. If key participants in the process (whether in production, consumption, trade, or, in this case, transportation) understand the power of a particular resource, then the resource’s owner can leverage it to threaten the process, potentially causing financial losses. Under such a threat, the owner demands a share of the product from the entire economic process in return. Prohibiting movement through certain territory can harm traders, and thus, territorial control can be effectively transformed into a resource.

How does this work? Let’s assume that, in Figure 10.2, goods need to be moved from point A to point C. The shortest route is ABC. But what if route AB is blocked by the owner of that territory? Then, alternative routes remain, for example, ADEBC or ADEFC. Each of these is, of course, longer and more costly than ABC. The question is only about which will be greater: the additional increase in costs or the payment demanded by the owner to unblock route AB.

In contrast to the Web-Model, where there is only one central point of control, which coincides with the place where profit is generated (from the sale of the delivered goods), the Net-Model has several control points, which typically don't coincide with the place where profit is generated, neither in time nor in space. This transforms the game between route owners into a cooperative one, though it remains competitive as well. In our example, profit may be generated at the final point C, while other routes and transport hubs can only claim a share of this profit by allowing goods to pass through their territory.

In an attempt to get his share, the owner of route AB may try to conspire with the owners of other potentially competing routes and hubs, but cooperation will require them to promise something in return. Such competitive-cooperative interactions automatically push relations between participants in the transport-logistics game beyond simple market transactions based on price compromise. In microeconomics, this situation is known as imperfect competition, characterised by a reduction in price competition and its replacement with non-price competition.

Geographical factors also reinforce the trend away from the model of perfect competition. Naturally, the number of truly accessible routes on land is significantly smaller than at sea. At sea, without much exaggeration, we can state that the potential number of routes equals the number of ship voyages, but on land, this is far from the case. By controlling territory, the owner can effectively restrict the free movement of goods. Thus, power shifts from the owners of vehicles (who are expectedly more numerous) to the owners of territories (who are naturally fewer in numbers). In microeconomics, this form of imperfect competition among a few suppliers is called an oligopoly (literally: 'few sellers'). It is known that under oligopoly conditions, the role of price competition diminishes, while the tendency towards collusion, mergers, and acquisitions intensifies.

In the Net model, junction points or transport hubs are of particular importance, as they allow control over several directions at once. By occupying an intersection, one can control several segments of the network with the same resources. This significantly enhances the efficiency of resource ownership. Of course, real landscapes are not as ideal as depicted in Figure 2. In reality, a hub may connect not only four but also three, or conversely, five or even more segments. The more routes a hub can potentially block, the better.

By negotiating with the owners of competing routes and hubs, or simply seizing or destroying them, one can achieve monopolistic power over transportation. This increases the benefits for the party that remains the dominant player. Such a windfall encourages territory owners to expand their control to neighbouring territories. Thus, competition is further reduced, and the model shifts from oligopoly to monopoly.

While reduced, the Net Model transforms into a transportation corridor, within which there is a single main supply line for goods without real alternative routes. Different stages of supply along the main route may belong to different owners. This model aptly describes the real situation of the Northern branch of the Great Silk Road, which stretched from the western regions of the Chinese empire through Central Asia to Eastern Europe, ending in Crimea. Throughout the journey, goods were transported by caravans, but no single caravan travelled the entire distance from China to Crimea, moving only part of the way and selling their goods to other traders who carried them further. Along the way, caravans passed through territories of various nomadic tribes, which participated in trade and provided protection, gaining certain benefits from the existence of caravan trade. Neighbouring tribes, therefore, competed for land for grazing and protection (or ‘protection’) of traders, yet they were interdependent, trying to maintain favourable and safe conditions for caravans. Thus, hostility had to be restrained within certain accepted boundaries (Fig.10.3).

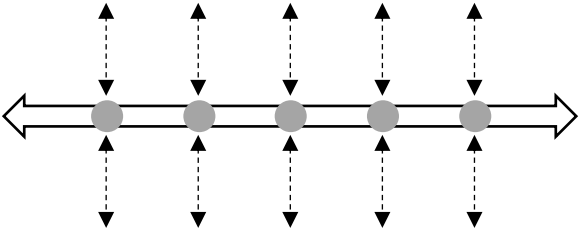


Fig. 10.3. Reduction of the Net-Model into a Transport Corridor

Overall, unlike the Web-Model, the Net-Model not only lacks perfect competition as an ideal reference. It does not have it at all due to the purely technical reasons outlined above. This results in fundamental differences in the perception of reality between people whose values are shaped by the Web model and those shaped by the Net-model. Some of the value orientations formed by the Web and Net-Models are presented in Table 10.1.

Even a superficial review of the values generated by the Web-model and the Net-model shows that they are not mutually exclusive. These values are quite compatible and can often lead to similar actions. However, the devil is in the details. Although we cannot directly see the values that guide other people, we can attempt to discern them through the judgments and subsequent decisions they make. This is precisely where inaccuracies, errors, and systemic manipulations may occur.

Table 10.1

Value Orientations of the Web-Model and of the Net-Model

Web-Model	Net-Model
Diversification strengthens	Unification strengthens
Inclusivity is a value.	Exclusivity is a value.
Power is when I am better than my competitors	Power is when my competitors are weaker than me
“Nature does nothing, humans do”	Territory, even uninhabited, has value

10.4. Strategy in the Net-Model: the Moscow case

Institutionalisation of the Net-Model leads to the spread of corresponding values within society, transforms communities accordingly, and shapes how decisions are made. While there is no absolute determinism in translating values into decisions and subsequent actions, societies and individuals tend to choose the most valuable (from their perspective) options when considering different possibilities. This ensures the logical coherence and consistency of chosen strategies and, ultimately, guarantees overall success, provided that the values align with reality.

An example of a successful strategy shaped by Net values can be seen in the rise of Moscow in Eastern Europe. For several centuries after its founding, Moscow remained a secondary, unremarkable town. Everything changed with the strategy that the Grand Duchy of Moscow (later the Tsardom, and eventually the Empire) began to implement around the second half of the 15th century. In a generalised and simplified form, the reasons for both Moscow's initially impoverished condition and its strategy for ascendance are explained in Fig. 10.4, which schematically presents the main trade routes in Eastern Europe.

Being in a gap in the transport and logistics network, Moscow was doomed to a miserable existence as a secondary state entity. This was the case until the end of another civil war for the Moscow throne. During the war,

Vasily II the Dark successfully seized the opportunity and defeated the Novgorod Republic, where his competitor was trying to hide. As a result, Novgorod agreed to sign an agreement on its partial dependence on Moscow and accept Moscow governors, formally remaining independent.

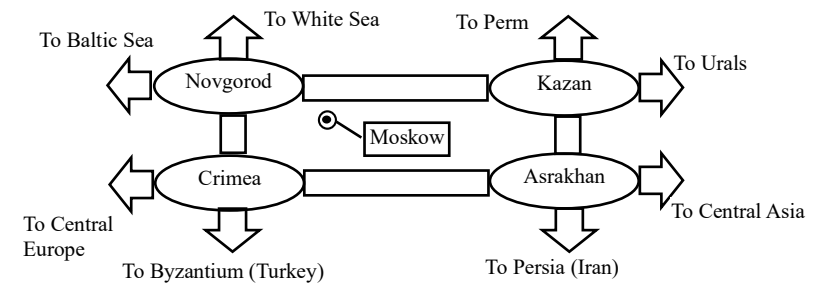


Fig. 10.4. Schematic Representation of the Net-Model for Eastern Europe

But even this partial control of trade significantly weakened Novgorod and, in return, gave resources to Moscow. This was the beginning of the implementation of a strategy of alternately capturing and destroying key nodes of the transport and trade network around Moscow. The implementation of the strategy took several centuries, but as a result, Moscow turned from a small settlement in the swamps into the undisputed hegemon of Eastern Europe and a country of pan-European importance. A brief idea of this strategy can be formed on the basis of the information presented in Table 10.2.

Noteworthy is the massacre that Moscow orchestrated in each of the cities it conquered. In Novgorod, according to Moscow’s own official accounts, the population was almost entirely exterminated or displaced and replaced by settlers from the Grand Duchy of Moscow. A similar fate befell Kazan. By the time of the campaign against Astrakhan, rumours of the Kazan massacre, along with the sight of mutilated, bloodied corpses of Kazan Tatars, which the Muscovites sent tied to wooden rafts down the Volga toward the then-independent Astrakhan Khanate, terrified the population. Alarmed, people abandoned their homes at the first rumours of the Muscovites’ approach, leaving Moscow’s army to find an entirely deserted city upon arrival.

The genocide of the Crimean Tatars extended over a longer period, as circumstances had changed, and the mass expulsion of the Crimean Tatars

was completed only in 1944 under Stalin's regime. Again, as in previous instances, thousands of Tatars were killed during the deportations, and those resettled in their place were people whose identity had been transformed into Russian generations prior.

Table 10.2

Stages of implementation of Moscow's strategy for obtaining a dominant position in Eastern Europe

Node	Time of conquest (approx.)	Consequence
Novgorod	1456 – 1478	Interruption of the Volga-Baltic route to weaken the Livonian Order in the Baltic and the Kazan Khanate on the Volga, conditions for further expansion to the White Sea region
Kazan	1487 – 1552	Weakening of the Astrakhan Khanate, conditions for further expansion to Perm, the Urals, and Siberia
Astrakhan	1552 – 1556	Isolation of Crimea, control of nomads near the Black Sea and the Caspian Sea; preparing a bridgehead for expansion into the Caucasus and later into Persia
Crimea	1700 – 1783	Significant weakening of Turkey; creeping expansion into Central Europe and the Balkans

The systematic genocide Moscow has repeatedly conducted over half a millennium is difficult to comprehend through Web-based values, yet it is readily explained through Net-based values. From a Web perspective, a territory devoid of human or even natural resources holds no value. However, from a Net perspective, even an uninhabited area has worth if it has logistical potential. It can be used to allow transit and earn revenue for one's own purposes, or it can be blocked if profits are higher elsewhere by diverting transport flows. Hence, genocide can prove to be quite profitable, though no less horrific. Moreover, the rational basis for genocide encourages its repetition as a successful business project – provided there are no internal or external constraints.

A critical part of Moscow's strategy to weaken neighbouring countries along the transport corridor in the Net Model has been and continues to be blockading. The method of such blockades is conveniently illustrated by examining Moscow's preparations for the attack on Ukraine. This assault, which began in 2014 and escalated to a full-scale invasion in 2022, was prepared well in advance, starting in 1992. The stages of preparation are presented in Table 10.3.

Table 10.3

Chronicles of Russian-Ukrainian gas conflicts

Year	Action
1991	After the collapse of the Soviet Union, Ukraine buys Turkmen gas, paying with industrial goods and food products; Kazakhstan and the Russian Federation act as transport intermediaries.
1992	The first verbal interventions regarding the need for Moscow to maintain control over the Ukrainian gas transportation network
1995	Suspension of gas supplies from Russia to Ukraine for the first time
2003	Moscow has blocked the transit of foreign gas through its territory; Russian gas tube operator "Gazprom" began to buy gas from Turkmenistan with a monopsony discount, and resells it to Ukraine with a monopoly markup.
2005	Moscow abuses power; "Gazprom" sets the price of Turkmen gas at \$44 and demands \$250 from Ukraine; thus, the brokerage margin is almost 470%
2009	Russia begins to actively block the supply of gas to Ukraine, demanding control over industrial, transport and military facilities; the construction of bypass gas pipelines begins.
2014	Russia starts the undisguised intervention; the Crimea, Donetsk, and Luhansk regions of Ukraine are occupied by Moscow.

In weakening its neighbours along the transport corridor by blocking supplies, Moscow, like any manipulator seeking to expand its area of control, must address the problem of finding alternatives. A neighbouring country concerned with Moscow's manipulations will try to find other supply routes. Within the Web-Model, this acts as an effective regulator against market power abuse; however, on land, it works far less effectively. If a port city-market benefits from freedom of movement by sea, on land, the number of viable alternatives rarely exceeds one or two, though even this limited choice can sometimes prove effective.

Moscow's strategy for effectively blocking logistical alternatives generally employs two approaches:

1. Conquest/Absorption of Competitors. This can involve either physical conquest or the acquisition of key infrastructural assets. The primary goal remains the same: to monopolise not only a specific logistics system hub but also nearby alternatives. Yet, seizing neighbouring network nodes does not fully solve the issue, as this establishes proximity to other previously distant nodes, which also need to be captured to reinforce monopoly power. As a result, Moscow's expansion is continually driven by internal motivations and never halts, except in cases of military defeat. A military defeat, of course, is not defined by loss of life (in the Net Model, human life

holds little value, almost none) but by loss of territory controlled by Moscow prior to the conflict.

2. Dividing the Neighbouring Society. This effectively involves bribing certain members of the business or political elite in the neighbouring transport-corridor country. These select partners are granted exclusive access to a blocked logistics resource in exchange for loyalty to Moscow. This practice has remained largely unchanged for over five centuries and is evident in the cases of some Tatar noble families who sided with Moscow during the conquest of Kazan, as well as certain European representatives who advocated for the construction of the Nord Stream and Nord Stream 2 gas pipelines. These chosen elite representatives do not always receive direct financial support from Moscow (although this is not uncommon). More often, the exclusive access to the logistics resource provided by Moscow allows them to realise monopolistic profits on purely market-based principles. This not only enables Moscow to finance its foreign agents without additional hassle but also weakens the neighbouring country's economy, laying the groundwork for further Moscow-led expansion. Essentially, pro-Moscow elites are allowed to occupy higher-ranking cabins on a sinking Titanic.

A special aspect of the strategy is combining Moscow's practices with Web-based values. The goal is to enable those with Web-based values to construct a coherent perception of reality, shaped by a society that is actually governed by completely different, Net-based values. Part of this is achieved through the universal transmitter of values – money – as we examined in the case of elite bribery. Specialists also play a critical role by portraying Russians as “human, too,” thus ensuring the continued work of “Putinverstehers” in the West. This includes diplomats, journalists, and members of the academic community. Finally, for those who physically visit Moscow, special entry points are set up to resemble a typical Web city with familiar attributes. Seeing familiar storefronts of global brands and hearing familiar phrases, Western visitors can easily convince themselves that, behind the scenes, lies a familiar picture – a large marketplace with a surrounding umland, though very expensive. Such an impression is precisely what visitors to Moscow and St. Petersburg are meant to experience. However, to Russians themselves, these entry points remain alien, particularly in terms of values. ‘There’s Moscow, and then there’s Russia’, they say, implying that the two are completely different worlds. A popular song characterises St. Petersburg, another showcase city for Western visitors, as a ‘pale, gaunt Euro-eyed passer-by’.

St. Petersburg is a particularly illustrative example of such a showcase. Outwardly, it looks entirely European. The central area contains docks for ships, a nearby stock exchange, an admiralty, and a palace. The city was deliberately built to resemble Amsterdam, but on a grander and more opulent scale. However, if a foreign visitor tries to peek behind St. Petersburg's elegant facade, they will see the leaden squalor of Russian life. Even in this case, a Web-minded visitor will not experience cognitive dissonance but will feel they're in an ordinary colonial port city like Havana or Santo Domingo, albeit unusually large, with Russia's territory from which colonial goods are exported, appearing vast compared to the Caribbean islands. However, this similarity is deceptive. Unlike real colonial port cities on coasts, what lies behind St. Petersburg is not just coffee and sugarcane plantations but an enormous world with entirely different values and a unique way of seeing the world. A wardrobe door and an apartment building door may look similar, but they are not the same thing.

There is nothing unique about Moscow's practices. They largely combine the practices of Central Asian nomadic states with Western trade and colonial practices. Yet, the longevity, scale, and resulting significance of these practices for Europe as a whole, and particularly for the Eastern European-Central Asian part of Eurasia, require a conscious approach to increase the effectiveness of working with Moscow.

10.5. Using the Net-Model to design a competitive environment in Eastern Europe

Understanding the differences between Net-values and Web-values can aid both in analysing past mistakes in Western interactions with Moscow and in formulating an effective Western strategy for the future. Without claiming an exhaustive list, let's provide a few examples of such errors:

1. *Not allowing Putin to win.* To this end, Ukraine was supplied with weapons, but in quantities and on a schedule that prevented Russian troops from facing decisive defeat or retreat. The most striking example is the delay in arms and ammunition deliveries from the U.S. in 2022–2023. An officially acknowledged NATO delay in the supply of arms and ammunition by four months allowed Russian forces to fortify previously captured areas in southern Ukraine, secure a land route to Crimea, and reliably cut off Ukraine's access to the Sea of Azov. In terms of Web-values, this outcome may hold little significance, but in the Net-values system, it is a major victory for

Moscow. Even if nothing else were to happen, the establishment of a land corridor to Crimea will be seen by Moscow as a massive national achievement whose value cannot be negated by any human or financial losses Moscow has already incurred or will incur in the ongoing war against Ukraine. In the Net-system, territory is a critical, enduring resource, while people and money are transient and, at best, secondary. To sacrifice secondary assets for a truly valuable gain is a real victory. Thus, if the American intent was to deny Putin a victory, this goal has failed disastrously.

2. *Making the cost of war unacceptably high for Putin.* This refers to financial losses (e.g., freezing Moscow's assets deposited in Western banks) or Russian military casualties on the battlefield. This approach cannot succeed, as it is based on Web-values. From the perspective of Net-values, financial losses can be easily compensated by re-establishing and strengthening monopolistic control over logistics. This can be achieved simply by capturing more territory. As for human losses, within Net-values, the population holds significant importance only when needed for territorial defence. This includes those directly involved in military actions or supporting military roles, such as in the military-industrial complex. All other people not engaged in these activities are of lesser value, and some categories are even considered burdens, better off removed, such as the unemployed or prisoners. If they die, it's even beneficial. Problems would arise only if losses became so large as to threaten the depletion of Russia's mobilisation reserve, leading to a physical inability to wage war. Given Russia's population size, this would mean tens of millions of people. Since Russian military losses remain pitifully low compared to the mobilisation reserve, claims of 'sanctions from hell' are seen by those holding Net-values as amusing but ultimately harmless eccentricities of Western politicians.

3. *Stopping hostilities to save lives.* This is, in fact, a double mistake. Firstly, within Moscow's worldview, human lives have little value. Evidence of this can be seen in the so-called 'meat assaults' in which Moscow sent its soldiers during World War I, World War II, and continues to send them now, attacking Ukraine. By sacrificing twice as many soldiers as the Armed Forces of Ukraine, Moscow gains small pieces of depopulated territory, yet clearly sees this practice as acceptable. Thus, rhetoric about preserving lives from Moscow's representatives is a clear manipulation. Secondly, within Moscow's value system, a ceasefire is nothing more than a way to lock in gains measured in square miles. History has shown that Moscow captures neighbouring states in successive wars, each time legitimising territorial

acquisitions incrementally. Over the past five centuries, nothing has ever cast doubt on the effectiveness of Moscow's strategy. Therefore, it would be unwise to expect Moscow to abandon a strategy that has proven consistently effective. The mistake is to believe that anything other than total battlefield defeat, including the loss of territories controlled prior to the war, will stop Moscow.

Recognising the ineffectiveness of current Western strategies toward Moscow opens the way to creating a more effective strategy, or at least identifying its key parameters. Clearly, as with any strategy, it should begin with an ideal vision of the future we aim to achieve. While such a vision is not set in stone, certain key features must be present. Among these features is the restoration of a healthy logistical structure in the Eastern Europe-Central Asia region. The necessity of transforming the current system of transportation corridors controlled by Moscow stems from the trend toward a reduction of a full-fledged transport network on land routes discussed earlier. This mirrors how a subject's behaviour in a market environment leads to reduced competition and the creation of a monopoly. Similarly, as with combating monopolisation, overcoming the reduction in Net-system competition can only occur through external forceful pressure. Such pressure poses challenges, as it targets not a private company but a nuclear-armed state. However, as in the case of market monopolisation, refusing to enforce competition leads to even worse consequences.

The ideal vision involves restoring a full network of routes in the North-South and West-East directions, something similar to the layout depicted in Fig.2, adjusted for geographic, ethnic, and demographic factors. Accordingly, this would be an area for broad discussion among experts from various fields, as well as representatives of ethnic communities. But as an initial model, the historical structure of trade routes in Eastern Europe before Moscow's hypertrophy (see Fig. 10.3) can be considered.

Moscow will fiercely resist such a scenario, as it would mean that the West has taken the situation seriously and moved from appeasement of the aggressor to a real attempt to address the Moscow problem.

References:

1. Biscaia R., Mota I., 2013, Models of spatial competition: A critical review, *Papers in Regional Science*, Volume 92, Issue 4, pp. 851–872

2. Fujita, M., Krugman, P., & Venables, A. (1999). *The Spatial Economy: Cities, Regions, and International Trade*. MIT Press.
3. Behrens, K., & Thisse, J.-F. (2007). Regional Economics: A New Economic Geography Perspective. *Regional Science and Urban Economics*, 37(4), 457–465.
4. Burger, M., van Oort, F., & Linders, G. J. (2009). On the Specification of the Gravity Model of Trade: Zeros, Excess Zeros and Zero-inflated Estimation. *Spatial Economic Analysis*, 4(2), 167–190.

Chapter 11
***Ukraine's contribution to human resource security and
reducing disparities in the European labour market***
(O. Zakharova)

Aggravating demographic challenges, population ageing, and imbalances between labour supply and demand have become serious issues for most countries worldwide. These problems are particularly acute in the countries of the European Union (hereinafter referred to as the EU), where workforce shortages in strategic sectors of the economy threaten to significantly slow innovation-driven development and reduce economic competitiveness in the near future. Such trends may substantially alter the global balance among key economic actors. The COVID-19 pandemic, the financial and economic crisis, and subsequently the war in Ukraine have further aggravated the socio-economic and humanitarian situation in Europe, triggering a redistribution of labour resources and significant changes in migration flows. In this context, workforce security in European countries is increasingly recognised as a critical component of national security. It encompasses preservation, development, and efficient utilisation of human capital and forms the foundation for partnership-based cooperation mechanisms among European countries across various sectors. These mechanisms aim to jointly and more rapidly address workforce imbalances in Europe. Thus, Ukraine's contribution to ensuring workforce stability and labour market balance in Europe has become exceptionally relevant and requires comprehensive academic analysis, which the chapter that follows seeks to provide.

11.1. Workforce security and labour market stability in eu countries: trends and challenges

In the contemporary global society, security issues have acquired exceptional importance for all countries, including those in Europe, due to a wide range of interrelated factors. These include heightened geopolitical tensions, escalation of armed conflicts in various regions, global economic volatility, and rapid technological change, all of which substantially affect the stability of socio-economic systems.

Alongside traditional dimensions of security, such as food, energy, environmental, and military, new dimensions are increasingly gaining prominence, among which workforce security now occupies a central position. Workforce security determines the ability of public authorities to meet the economy's demand for qualified specialists and talent, prevent human capital outflows, foster innovation across all spheres of human activity, and sustain economic development at both regional and national levels.

Over the past 20 years, most EU countries have experienced a gradual decline in fertility rates, while mortality rates have remained relatively stable, with a slight upward tendency (Fig. 11.1). This relative demographic stability has been achieved through adequate income levels, access to high-quality nutrition, advanced healthcare services, well-developed social infrastructure, and effective healthcare systems across all 27 EU member states. These factors indicate a certain adaptability of demographic processes to the socio-economic conditions of individual countries.

In 2006, the highest crude birth rate was recorded in Ireland (15.3‰), while the lowest was observed in Germany (8.2‰) [1]. By 2024, the situation had changed: Cyprus reported the highest birth rate (10.2‰), whereas Italy recorded the lowest (6.3‰). This clearly demonstrates a sustained downward trend in the number of live births per 1,000 inhabitants across the EU during the analysed period, which constitutes one of the most powerful drivers of accelerated population ageing.

Regarding mortality dynamics, in 2006 the highest crude death rate was simultaneously observed in Latvia and Bulgaria (14.9‰), whereas Ireland recorded the lowest rate (6.7‰). By 2024, the situation had changed only marginally: Latvia still exhibited the highest mortality rate (14.3‰), and Ireland again maintained the lowest level (6.5‰). Overall, peak mortality rates showed a slight downward trend during the study period, which is a

positive tendency.

Notably, Ireland stands out among EU countries for having one of the most favourable demographic situations, combining the lowest mortality rate with one of the highest birth rates (10.0‰ in 2024, significantly above the EU average). This warrants further in-depth research of the demographic context in Ireland to identify the set of factors that contributed to such positive outcomes and to explore the potential transfer of this experience to other EU member states.

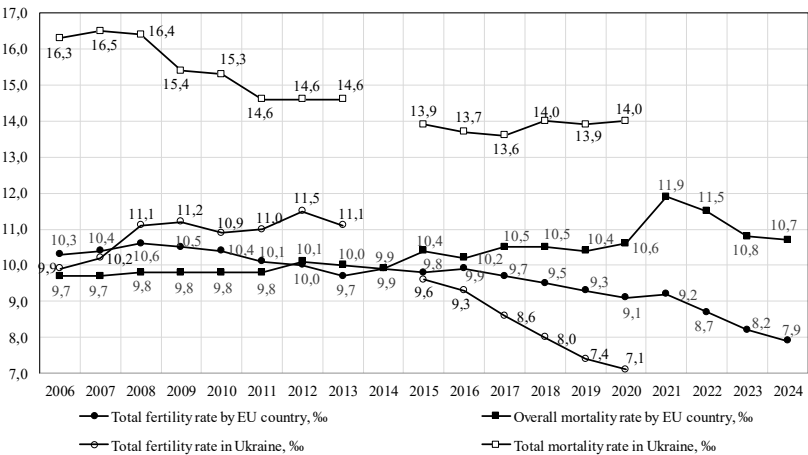


Fig. 11.1. Dynamics of crude birth and death rates in EU countries and Ukraine, 2006–2024, ‰

Source: compiled from [1]

Since 2014, the EU has experienced a negative demographic phenomenon long familiar to Ukraine throughout its independence: annual mortality exceeding fertility, with the gap between these indicators widening over time. This dynamic underlies adverse changes in the age structure of populations and ultimately leads to an intensification of population ageing, which is a minatory tendency [2]. However, active migration policies and attracting young workers from partner countries have partially offset labour shortages in the EU, helping to maintain labour market stability and support sustainable economic development in the member countries.

In contrast, prior to the russian invasion, Ukraine exhibited higher

fertility rates than the EU (e.g., 11.5 births per 1,000 inhabitants in Ukraine versus 10.0 in the EU in 2012), but also significantly higher mortality rates and a much larger excess of deaths over births. This reflects substantial disparities in living standards and the ineffectiveness of Ukraine’s social policy. Over the entire period of independence, these trends represent an even more severe challenge than population ageing, namely, depopulation [3; 4; 5]. Over the past eleven years, due to the war, this trend has reached catastrophic proportions, and effective solutions have yet to be found.

The excess of mortality over fertility in EU countries since 2014 resulted in negative values of natural population growth (Fig. 11.2). From 2020 onward, annual population decline exceeded 1.1 million people, peaking at 1.28 million in 2022. While such dynamics would be irreparable for Ukraine, their impact on the EU’s total population was relatively limited, causing but a slight decline in 2021–2022 (Fig. 11.3). Subsequently, population growth trends resumed in the EU, largely due to a strong “demographic resilience” supported by high living standards, which continue to attract migrants from other countries, including Ukraine.

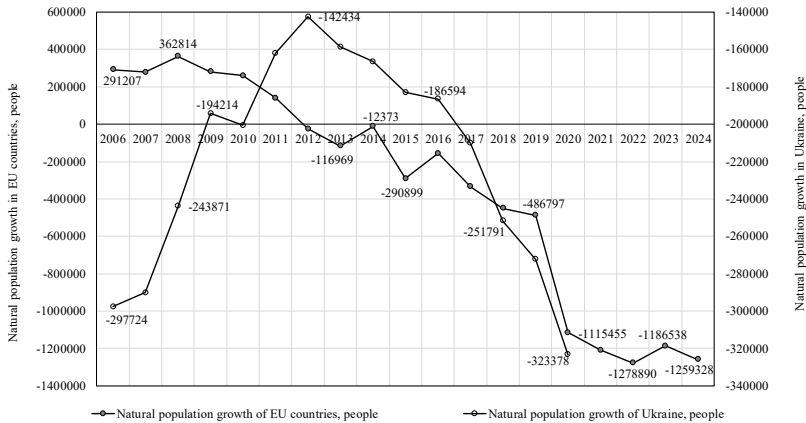


Fig. 11.2. Natural population change in EU countries and Ukraine, 2006–2024, persons

Source: compiled by the author based on [1]

Although most EU countries demonstrate low though relatively stable population growth, overall population expansion has been made possible by

proactive migration policies, robust family support systems, and effective demographic incentive programmes. Despite ongoing population ageing, EU countries have avoided sharp population decline through successful integration of labour migrants, including those from Ukraine.

Ukraine, by contrast, continues to experience a negative demographic trajectory, further widening the gap with European countries in terms of population recovery. While the natural population decline initially showed some improvement almost halving the gap between the number of births and deaths, from 2012 onward the situation deteriorated significantly. On the eve of the full-scale invasion, natural population decrease exceeded even the lowest levels recorded in 2006. This has directly contributed to a sustained decline in Ukraine’s total population throughout the analysed period. Population decline in Ukraine is driven not only by demographic factors but also by intensified migration processes, large-scale labour emigration, and wartime losses among both military personnel and civilians.

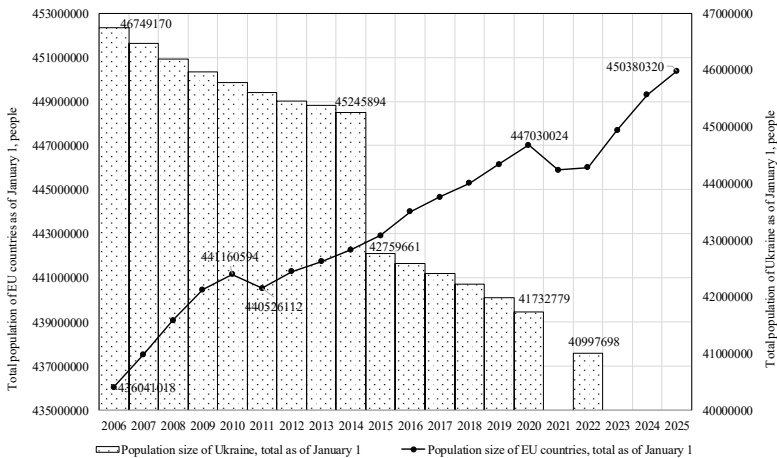


Fig. 11.3. Population size in EU countries and Ukraine, 2006–2025, persons

Source: compiled by the author based on [1]

This situation poses serious challenges to the preservation of labour potential, the functioning of social infrastructure, and the maintenance of economic growth in the country, both during wartime and in the post-war period. Against this background, the experience of European Union countries

appears particularly instructive. Through well-designed demographic, social, and migration policies, EU states have managed to stabilise the size of their permanent population and, in some cases, even achieve gradual population growth over time, despite external shocks and force majeure circumstances. For this reason, the European model of managing demographic processes may be highly relevant for Ukraine in the context of developing post-war recovery strategies and strengthening national workforce security.

An important component of a country's workforce security is the age structure of the population in a given territory, which determines the ratio between the working-age and non-working-age population. This structure can be characterised by the dynamics of the age dependency ratio, a key indicator and marker of regional social resilience. Various methodological approaches may be deployed to calculate this indicator; however, this study adopts the classical definition – ratio of the population aged 0–14 and 65 and over to the population aged 15–64 (Fig. 11.4). In our view, this ratio provides the most objective picture of population age structure, labour potential, and the level of social burden placed on the economically active population. Such an approach enables a comprehensive understanding of demographic ageing, workforce reproduction, and the capacity of the national social security system.

Throughout the entire study period, the age dependency ratio in EU countries exceeded 50 dependants per 100 working-age individuals and demonstrated a stable upward trend, although the pace of growth has slightly slowed in recent years. This level is relatively high and, in most cases, exceeds the corresponding value observed in Ukraine. The increase is primarily driven by population ageing and the growing share of elderly people in the total population. If the growth of the indicator were driven by an increase in the population aged 0–14, such dynamics could be considered positive, as they would create a strategic foundation for long-term workforce reproduction and sustainable demographic development. However, in the EU context, the rising dependency ratio is largely the result of population ageing, which intensifies pressure on social systems and pension funds.

Indeed, according to 2024 data, EU countries have approximately 1.76 employed persons per one social dependant, creating significant strain on pension systems, healthcare services, and the social care sector. The continued increase in this ratio over time reflects persistent ageing trends, as the elderly population grows faster than the working-age population. This situation necessitates the activation of employment-support policies, efforts

to extend the working lives of older individuals, and the attraction of labour migrants to maintain economic balance [6]. At the same time, a regulated level of immigration allows the EU to partially offset labour shortages, supporting workforce renewal and productivity growth across economic sectors. Consequently, achieving and maintaining an optimal balance between working-age and non-working-age populations should be regarded as a key objective of EU workforce and socio-economic policy in the coming years.

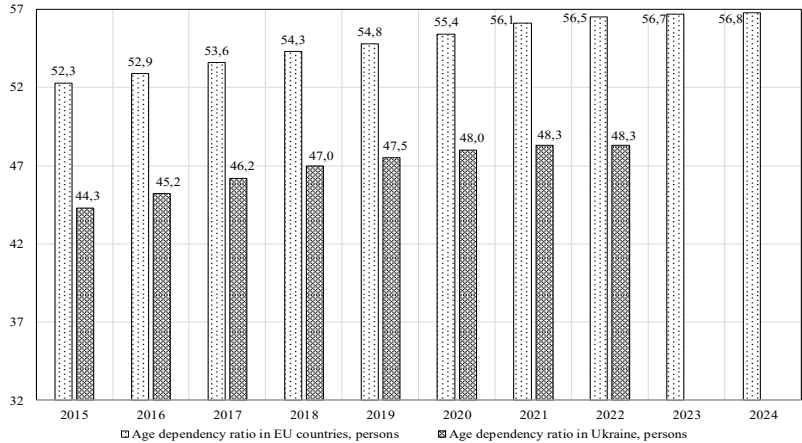


Fig. 11.4. Dynamics of the age dependency ratio for EU countries and Ukraine, 2015–2024 (persons)

Source: compiled by the author based on [1].

In Ukraine, the age dependency ratio exhibited a persistent upward trend over the study period, increasing from 44.3 to 48.3 persons. This negative dynamics is driven by a declining share of young people and the outflow of the working-age population, highlighting the urgency of regulating workforce balance at both national and regional levels. Demographic and labour market conditions have further deteriorated due to internal displacement, emigration in search of safer living conditions, and other objective factors. An additional threat contributing to the rising dependency ratio is the increased mortality among the working-age population, children, and youth as a result of ongoing shelling of civilian cities by the Russian Federation, military casualties at the front, and heightened morbidity and mortality caused by prolonged exposure

to severe stress. In 2024 alone, the number of births in Ukraine was three times lower than the number of deaths, significantly worsening the country's demographic situation. As a result, Ukraine's labour market is already experiencing a substantial shortage of human resources, particularly highly qualified personnel, which may pose a serious risk to the implementation of post-war economic recovery programmes.

Thus, the analysis of various components that collectively form the foundation of workforce security, using EU countries as an example, allows us to conclude that European labour policy is systemic in nature. Its effectiveness is ensured by a well-balanced combination of demographic, educational, social, and migration instruments aimed at maintaining equilibrium between economic needs and labour market capacities.

Today, European countries demonstrate an effective model of workforce stability based on long-term strategic workforce planning, a high level of social protection, and the stimulation of inflows of intellectual capital from countries with lower levels of economic development. However, relying exclusively on external labour inflows in the long term is risky. Therefore, internal workforce reproduction programmes are required, focusing on increasing birth rates among the native population, providing effective support to families with children, developing vocational education and retraining systems, and promoting lifelong learning. Special attention should be devoted to encouraging youth participation in the labour market, expanding opportunities for women, and integrating older persons and veterans into productive activities through flexible employment arrangements and intergenerational knowledge transfer [6].

Such measures can reduce dependence on external labour migration and enhance labour market resilience during periods of significant demographic fluctuation. Moreover, investment in internal human capital development will strengthen innovation capacity and improve the global competitiveness of the European economic area. In this context, the EU experience may serve as a valuable reference for Ukraine in building its own workforce security system based on balanced development, inclusiveness, and strategic planning based on anticipating the economy's demand. However, for such a system to be successfully implemented in Ukraine, it is essential to end hostilities, guarantee safety across all regions, and substantially improve living standards, which will create conditions that would facilitate, in the first place, the return of Ukrainian citizens who have left their homes due to various

factors and, secondly, will attract foreign residents to consider Ukraine as a country for a stable and prosperous future [7].

Unfortunately, this remains a vision for the future. At present, Ukraine has become one of the key donors of valuable labour resources to the European labour market, significantly influencing workforce security and labour market stability in EU countries. The mass forced migration of Ukrainian citizens caused by military aggression has filled labour shortages in several critical sectors of European economies, from services, agriculture, and logistics to healthcare, education, and information technology. This inflow of labour has played a crucial role in maintaining the functional resilience of European economies, particularly during post-pandemic recovery and rising demand for skilled workers. Ukrainian employees, widely recognised for their discipline, strong workplace ethics, high qualifications, and adaptability, have contributed substantially to productivity and economic stability in host countries. Moreover, the relatively high educational attainment of Ukrainian specialists has strengthened the intellectual and technological capacity of receiving states. At the same time, the Ukrainian diaspora has acted as a catalyst for intercultural and professional linkages, fostering the emergence of a shared labour space between Ukraine and the EU.

11.2. Ukraine as a strategic partner of the eu in ensuring workforce security and demographic resilience

Labour migration, as a socio-economic phenomenon, affects host regions and donor regions in different ways. Countries belonging to the first group generally benefit from labour migration through access to sufficient volumes of low-cost labour, filled vacancies in low-prestige and physically demanding jobs, GDP growth, increased household incomes, and reduced social tension. In contrast, donor countries face negative consequences such as a decline in the economically active population, reduced innovation capacity, critical shortages of specialists in vital sectors, and deteriorating quality of governance due to the emigration of qualified youth, experienced professionals, and researchers. These outcomes also reflect the loss of returns on investments in human capital and its gradual depletion for the national economy [3].

Ukraine belongs to this second group of countries. Its economy has long been affected by deep socio-economic, financial, and political crises

stemming from ineffective and unstable governance, widespread corruption, demographic decline, and a weak innovation strategy. As a result, many highly qualified working-age individuals have perceived employment abroad as the only viable strategy for ensuring stable living conditions for their families, thereby limiting Ukraine's potential for human capital growth.

In a generalized form, twelve key criteria can be identified that influence an individual's decision to emigrate: marital status, availability of decent employment and working conditions, ownership of real estate, possession of movable property, level of education and the prestige of the diploma obtained, health status of the individual and family members, opportunities for high-quality annual recreation, the ability to ensure an adequate level of education and healthcare for oneself and one's family, professional ambition, capacity to satisfy consumer needs, and, finally, the availability of financial savings for unforeseen circumstances [3; 7]. Naturally, this list may be expanded; however, these factors define the fundamental framework within which individuals make life-trajectory decisions that underpin trends in the accumulation of both personal and societal human capital.

The issue of population outflow for temporary or permanent residence abroad became particularly acute following the onset of the full-scale military invasion of Ukraine by the Russian Federation on February 24th, 2022. As a result, approximately 8.3 million people fled to European countries as refugees, the majority of whom were women and children (as of mid-2022, women accounted for 86.0% of all Ukrainian war migrants) [8; 9]. Throughout the war, the number of Ukrainian war migrants fluctuated due to simultaneous processes of departure and return driven by various subjective and objective factors. As of early October 2025, 5,752,670 Ukrainian war migrants remain in Europe [10]. The largest host countries as of September 1st, 2025, were Germany (1,233,280 persons), Poland (1,006,900 persons), and the Czech Republic (397,250 persons) [10].

The prospects for rapid economic recovery and infrastructure reconstruction in post-war Ukraine will largely depend on whether Ukrainian citizens return during the cessation of hostilities. However, even under optimistic scenarios developed by experts at the M.V. Ptukha Institute for Demography and Social Studies, no more than 50.0% of Ukrainian war migrants are expected to return. Even this relatively low return rate indicates an imminent and severe shortage of national labour resources in Ukraine's labour market following the end of the war. Should only 20.0-30.0% of migrants return – which is highly plausible – the government must already

begin implementing comprehensive programmes to stimulate repatriation. Such programmes should combine economic and social reintegration mechanisms, including housing provision, job creation, tax incentives for returning entrepreneurs, professional adaptation schemes, and psychological support.

Equally important is the development of regional infrastructure and improvements in quality of life at the community level, ensuring that return becomes a conscious choice rather than a forced necessity. Additionally, conditions must be created to engage the Ukrainian diaspora in economic recovery, including investment in local businesses and participation in joint educational and research initiatives. This approach would not only compensate for workforce losses but also transform migration into a driver of human capital development and economic renewal.

Indeed, despite its devastating consequences, the full-scale war in Ukraine has resulted in Ukrainian human capital becoming a significant factor in strengthening labour security within the European Union. Millions of Ukrainian professionals have contributed to the continuity of production processes, stability of service sectors, and functioning of social systems across EU countries [11].

Moreover, their contribution is not merely quantitative but also qualitative: Ukrainian migrants, through their professional culture and adaptability, enhance efficiency and innovation in European economies. This phenomenon is shaping a new model of workforce interaction between Ukraine and the EU, grounded in solidarity, mutual benefit, and the integration of human potential into a unified European space.

A distinctive feature of the current migration wave from Ukraine is its gender-age composition: the overwhelming majority of migrants are working-age women and children. This structure is largely the result of mobilisation restrictions that kept men in Ukraine. In the short term, this has helped EU countries partially reduce age-dependency ratios, as working-age women entered labour markets and integrated actively into host economies. At the same time, the demographic structure of EU populations has been rejuvenated through the arrival of young Ukrainian families and children, creating potential for future natural population growth.

In the long term, this trend is expected to strengthen Europe's labour potential by combining education, mobility, and high adaptability among Ukrainian migrants. In addition, the participation of Ukrainian women in economic activity contributes to improving gender balance and increasing

employment in sectors requiring strong communication and social competencies. Thus, forced migration from Ukraine, despite its tragic origins, has become a factor of positive demographic transformation and enhanced labour resilience in EU countries.

At the same time, the war in Ukraine has generated positive shifts not only in EU labour security but also in European economic development more broadly, despite the substantial financial assistance provided to Ukraine and its refugees. Poland offers a clear example of this impact [12]. Ukrainian refugees have strengthened sectors such as construction, logistics, transport, and services by often performing work considered unattractive by local workers. During the first two years of the war, Ukrainians in Poland established 59.8 thousand private enterprises and businesses, creating jobs for both their Ukrainian countrymen and Polish citizens. According to official estimates, Ukrainian war migrants contribute between 0.5% and 2.4% to Poland's GDP annually, with a stable upward trend.

Thus, Ukraine has made a tangible contribution to ensuring Europe's labour security by providing its most valuable resource, namely, human capital, which has supported labour market stability and facilitated socio-economic integration and humanitarian cohesion across the continent. Given the protracted nature of the war, this contribution is strategic rather than short-term: Ukrainian professionals are becoming an integral part of a new European economic architecture based on mutual support, solidarity, and shared responsibility for human capital development. While Ukraine faces population losses due to war and labour migration, EU countries benefit demographically and in workforce capacity, strengthening labour market stability, which is an essential factor in global competitiveness.

For Ukraine, participation in European labour markets also offers opportunities to reduce unemployment and enhance the quality of domestic human capital through professional development programmes, internships, and academic mobility. This interaction fosters the formation of a shared workforce space characterized by the exchange of knowledge, skills, and management practices.

At the same time, large-scale labour migration requires the Ukrainian state to develop mechanisms for retaining intellectual potential and stimulating the return of specialists after they acquire European experience. This issue is particularly sensitive for both Ukraine and EU countries hosting Ukrainian war migrants. Without large-scale return migration, rapid post-war economic recovery in Ukraine will be difficult; conversely, EU countries are

not interested in losing migrants who have already integrated into local labour markets, enrolled their children in schools, and established stable livelihoods.

This creates a complex dual-interest dilemma: Ukraine needs the return of its human capital for reconstruction, while EU countries seek to preserve it to maintain labour stability. In the long term, this may lead to a new model of cross-border labour mobility in which Ukrainian professionals remain part of the European labour space while maintaining strong ties with their homeland.

A step in this direction would be for the government to approve dual citizenship for Ukrainian citizens. Accordingly, it is essential to develop bilateral partnership mechanisms between Ukraine and the EU aimed at the mutually beneficial realization of Ukrainian workforce potential and support for post-war recovery processes [13]. Thus, workforce security acquires strategic importance not only at the national but also at the continental level, as labour market stability is a fundamental prerequisite for economic growth and social cohesion within the European Union.

References

1. Population change - Demographic balance and crude rates at national level. Eurostat. Available at: https://ec.europa.eu/eurostat/databrowser/view/DEMO_GIND_custom_18412266/default/table
2. Zakharova, O., Lopushniak, H., Skibska, K. (2022). Current trends in the development of Ukrainian labor market. *Studia Regionalne i Lokalne*, No. 3(89), pp. 17–31. <https://doi.org/10.7366/1509499538902/>
3. Zakharova, O. V. (2020). Ukraine's loss of human capital due to demographic, socio-economic and socio-political crises, 1990-2019. *Revista Galega de Economía*, Vol. 29, No. 2, pp. 1–14. <http://dx.doi.org/10.15304/rge.29.2.6872>
4. Захарова, О. В. (2020). Тенденції нагромадження людського капіталу в Україні за період незалежності. 36. наук. праць Черкаського державного технологічного університету. Серія: Економічні науки. Вип. 59. С. 85–97. <https://doi.org/10.24025/2306-4420.1.59.2020.222098>
5. Захарова, О. В. (2018). Демографічне старіння населення: наслідки та перспективи для України. *Наукові записки Національного університету «Острозька академія»*. Серія «Економіка»: наук. журнал. No. 9(37). С. 11–15. [https://doi.org/10.25264/2311-5149-2018-9\(37\)-11-15](https://doi.org/10.25264/2311-5149-2018-9(37)-11-15)

6. Захарова, О. В. (2018). Потенціал людини третього віку для суспільства. Зб. наук. праць Черкаського державного технологічного університету. Серія: Економічні науки. Вип. 49. С. 26–33. <https://doi.org/10.24025/2306-4420.0.49.2018.136140>

7. Захарова, О. В. (2019). Умови повернення трудових мігрантів в Україну. Зб. наук. праць Черкаського державного технологічного університету. Серія: Економічні науки. Вип. 55. С. 15–23. <https://doi.org/10.24025/2306-4420.0.55.2019.185954>

8. Зменшення народжуваності, міграція та смертність: як Україна відновлюватиме демографічний рівень. Kyiv Post Ukraine's Global Voice. Available at: <https://www.kyivpost.com/uk/post/31481>

9. Якість життя населення України та перші наслідки війни / Черенько Л. М., Полякова С. В., Шишкін В. С., Реут А. Г., Крикун О. І., Когатько Ю. Л., Заяць В. С., Клименко Ю. А.; Нац. акад. наук. Укр., Ін-т демогр. та соц. дослідж. ім. М. В. Птухи. Електронне видання. Київ, 2023. 191 с. Available at: <https://idss.org.ua/arhiv/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F%D1%8F%D0%BA%D1%96%D1%81%D1%82%D1%8C.pdf>

10. Ukraine Refugee Situation. Operational data portal. Available at: <https://data.unhcr.org/en/situations/ukraine>

11. Ринок праці України 2022–2023: стан, тенденції та перспективи / Судаков М., Лісогор Л. Звіт. Державна служба зайнятості України, Федерація роботодавців України, Міністерство освіти і науки України, Європейський банк реконструкції та розвитку, Фонд міжнародної солідарності (Solidarity Fund PL), 2023. 170 с. Available at: https://solidarityfund.org.ua/wp-content/uploads/2023/04/ebd_ukraine-lm-1.pdf

12. BGK: Wpływ migrantów z Ukrainy na polską gospodarkę. 2025. Available at: <https://www.bgk.pl/aktualnosc/bgk-wplyw-migrantow-z-ukrainy-na-polska-gospodarke-1/>

13. Глобальні трансформації трудових ресурсів та забезпечення міграційного дискурсу: монографія / С. П. Калініна, С. П. Ланська, В. В. Подунай, В. В. Воскобойник; за заг. ред. С. П. Калініної. Вінниця: ТВОРИ, 2025. 220 с. Available at: https://repository.mu.edu.ua/jspui/bitstream/123456789/9371/3/glob_prob1_trudor_zabezp_monog_2025_1.pdf

Section 3

Economic Security of Europe and its Components

Chapter 12

Economic security as an institutional prerequisite for the innovative development of society

(Y. Petrunia, T. Pasichnyk)

In today's environment, humanity is facing many security challenges that were not so obvious or did not manifest themselves with such acuteness before. Military conflicts, epidemics, social unrest, and trade wars outline the contours of a new reality and form new requirements for security architecture. In such circumstances, it is becoming increasingly clear that social development and economic growth – the necessary conditions for improving people's well-being – cannot remain exclusively in the realm of economic discourse or be reduced to purely economic reforms. Without ensuring basic security conditions, it is impossible to count on long-term economic growth. That is why it is becoming increasingly important to consider economic security as an institutional prerequisite for innovative development of society, which is the subject of this chapter.

12.1. Innovation as an integral feature of economic development

At an intuitive level, the idea of a close connection between innovation and economic development is perceived as obvious. This notion has deep philosophical roots that go back to the ancient tradition, and in modern times it took on a new form in optimistic concepts of technological progress as a driver of social change. In particular, in F. Bacon's utopian work '*New Atlantis*' (1627) [1], scientific knowledge appears as the basis of an ideal social order.

The foundation for the philosophical understanding of technology was laid in the work of E. Kapp '*Updates to the Philosophy of Technology*' (1877) [2], which is considered the beginning of the formation of a separate direction – the philosophy of technology. In this work, technical means (including tools

and weapons) are interpreted as ‘projections’ of human organs, i.e. external materialization of bodily functions. Thus, it is demonstrated that technology expands the boundaries of human capabilities, being rooted in corporeality and subjective human experience.

In the first half of the twentieth century, a number of influential thinkers – M. Heidegger, J. Dewey, H. Arendt, H. Marcuse, G. Anders, and others – paid great attention to analyzing the role of technology in the modern world. They unanimously recognized that technology has become a central component of social life, while emphasizing its ambivalent nature. Philosophical reflections are dominated by critical reflection on both the potential dangers and opportunities offered by technological progress. These problems were particularly deeply elaborated in M. Heidegger's work *‘The Question of Technology’* (1954) [3], which deals with the hidden nature of technology and its ability to transform the way of human existence.

Since the end of the nineteenth century, in particular in the works of T. Veblen, the approach known as technological determinism has gradually emerged in the scientific and philosophical literature – a concept that gives technological progress the status of the main factor of historical change and social evolution. In its most radical form, this theory assumes that technology develops independently of social influence, and that all significant social changes are a direct consequence of technical innovation, ignoring interaction with political, cultural, and institutional factors. According to T. Hauer, radical technological determinism views technology as an autonomous force independent of human will that determines the course of social change [4]. This approach assumes that technological progress is a priori positive and inevitable, and that social choice regarding the directions of its application is secondary.

In our opinion, the philosophy of technological determinism is conceptually embedded in the neoclassical theory of economic growth, in particular in the model of R. Solow and T. Swan (1956). In this model, technology is viewed as a public good – an exogenous factor that provides a universal and almost automatic impact on economic growth. This approach assumes that technological progress is the main driver of development, independent of the social or institutional context.

In contrast to the hard version of technological determinism, soft determinism recognizes the leading role of technology, but emphasizes the importance of the social environment, which determines how these technologies are adapted, used and developed. In particular, A.

Gershenkron, J. Schumpeter and their followers took a more cautious position. They argued that the process of technological catching up is not automatic and requires deliberate efforts, institutional reforms, and an appropriate organizational environment. A central theme in the scientific literature on this issue is the concept of "capabilities" that must be created at the level of enterprises, industries and national economies to avoid the trap of underdevelopment [5, p. 2]. In other words, the availability of advanced technologies alone does not ensure development without proper social and institutional support.

Since the middle of the twentieth century, criticism of the idea of technological determinism has grown, especially in the context of the ethical and social consequences of technological progress. The social construction of technology (SCOT) approach, proposed by W. Biker, T. Hughes, and T. Pinch (1987) [6], questioned the idea of technological determinism and considered technology not as an autonomous force that shapes society, but as a product of interaction between social groups, political interests, cultural norms, and institutional structures. According to this concept, it is society that determines what technologies emerge, how they are implemented, and what they are used for. In other words, technological development is not a deterministic factor but a socially embedded process that depends on the action of formal (laws, policies, norms) and informal (traditions, values, social perceptions) institutions. One of these critical institutional factors is the system of ensuring the economic security of the state, which affects the ability of society to create innovations and respond to the challenges posed by new technologies.

Recognizing the social nature of technologies destroys the idea of their neutrality and emphasizes the responsibility of society for the selection, development and application of technical solutions. This means that innovations are neither a priori useful nor inevitable – their impact depends on the context in which they are realized and on the existence of mechanisms that facilitate their implementation.

Regardless of whether we accept the concept of technological determinism (in its radical or mild version) or follow the approach of social construction of technologies, modern economic thought is actually based on the assumption that development – social or economic – is impossible without technical knowledge and innovation. The idea of innovative development has become dominant, and innovativeness is almost a normative requirement for any model of progress. Today, innovation is seen not as one of the possible

ways of development, but as its undeniable imperative. However, the question arises: is development really possible without innovation? Do we have any reason to believe that any progress must be innovative in nature?

The fact that innovation is perceived as an essential feature of development is the result of several historical, intellectual and methodological shifts:

- first, since the Enlightenment, and especially after the Industrial Revolution, the idea that social progress is equated with technological progress has been entrenched in European thought. Increased productivity, rationalization of labor, secularization, and scientific and technological discoveries were seen as markers of modernization, and thus of development itself. Although this connection was not always direct, it formed the basis of optimistic conceptions of development in which technology was the main driver of change;

- secondly, in the twentieth century, this concept was analyzed in economic theory. The works of J. Schumpeter, who introduced the concept of innovation as a driving force for economic development [7], R. Solow, who demonstrated the contribution of technological progress to economic growth [8], the theories of human capital by T. Schultz [9] and G. Becker [10], and many other representatives of economic thought have consolidated the belief that sustainable development is impossible without technical and organizational innovations. Technology has gradually turned from one of the factors of production into a key determinant of economic success;

- third, since the second half of the twentieth century, especially since the 1980s, international organizations (World Bank, OECD, UN) have been popularizing the concept of "innovation economy", where scientific research, new technologies, innovations and education have been considered as the main indicators of 'developed' countries. Strategic documents often directly equate the concepts of 'economic development' and 'innovative development' [11]. For example, in the reports of the OECD or the European Commission, indices of innovation capacity are directly related to long-term growth forecasts. As a result, in both academic and political discourse, the concept of development has become almost automatically associated with economic growth, technological modernization, and innovation. This approach somewhat displaces alternative interpretations of development, such as improving the quality of life, cultural improvement, social justice, etc. The danger is that the value-based vision of development is being

replaced by a technocratic paradigm in which development is understood exclusively as technological improvement.

If we consider innovations as a factor that influences the process of economic development, there is a need for a deeper analysis of the nature of this influence. On the one hand, a number of empirical studies confirm the positive relationship between the level of innovation activity and economic dynamics. On the other hand, the literature has accumulated a lot of evidence that innovations do not always generate the desired socioeconomic effect and may, on the contrary, exacerbate structural problems. Some researchers explain this ambivalence by the low efficiency of innovation implementation and scaling, rising unemployment due to automation and robotization of production, deepening income inequality due to unequal access to innovation, monopolization of R&D results by large technology companies, etc.

To understand the mechanisms of innovative development, the works of C. Freeman and B.-A. Lundvall – the founders of the theory of national innovation systems – are of great importance. They emphasize that the success of innovation activities depends not on the isolated action of individual elements, but on the coordinated functioning of the entire system as a whole. They pay special attention to the role of the state innovation policy designed to create a favorable institutional environment for the development and implementation of innovations. According to the theory of innovation systems, institutions have a decisive influence on their formation – in particular, laws, regulatory and cultural norms, standards that can both stimulate and restrain the innovation process [13, p. 5–6].

The following quote from the work of D. North and R. Thomas can serve as a generalization of the above theoretical approaches: *‘The factors we have listed (innovation, economies of scale, education, capital accumulation, etc.) are not causes of growth; they are growth’* [14, p. 2]. In view of the above, key questions arise: if we identify innovative development with economic development, recognizing the technological component as its organic and integral part, and share the philosophical position of the social construction of technologies, what factors are the fundamental determinants (driving forces) of innovative development? What is it at the macro level that determines not only the emergence of new technologies but also their successful adaptation, dissemination, and impact on socio-economic processes?

To answer these questions, it is not enough to focus exclusively on the analysis of the mechanics of economic growth – that is, on the direct variables

that allow us to model its dynamics. Thus, according to D. Acemoglu, there are direct factors that determine the mechanics of economic growth and are necessary for building formal models, as well as fundamental factors of development that form the preconditions for development, which are difficult to formalize, but they explain why countries with similar resource potential show different results in economic development [15, p. 110].

The direct factors of growth – natural resources, labor, capital and technology – are known from the works of classical political economy. At the same time, there is no unanimity in the scientific community regarding the fundamental causes: economists, historians, and sociologists offer different explanations. D. Acemoglu identifies four key hypotheses that explain the fundamental factors of economic growth [15, p. 110]:

1) ***the hypothesis of chance***. It is assumed that countries with similar initial conditions can follow different development trajectories due to random events or decisions made at critical points. This hypothesis resonates with the provisions of the general theory of complex systems, which states that random fluctuations play a key role near the bifurcation point, while between them deterministic factors dominate [16, p. 215];

2) ***geographical hypothesis***. Geography refers to all natural factors that affect humans as part of the ecological environment. They can also determine the trajectories of economic growth: the availability of resources affects the productivity of industry, climate and soil quality affect agriculture, topography affects logistics and communications, and so on. Some studies also link climate to people's propensity to save and to consume earlier or later. Thus, the geographic hypothesis is well integrated into formalized models of economic growth;

3) ***cultural hypothesis***. This is a system of beliefs, values and preferences that influence the economic behavior of an individual [15, p. 111]. It should be viewed more broadly as a hypothesis about informal institutions, which covers differences in religious beliefs, national cultures, language, education, social stratification, mobility levels, etc. These factors determine the readiness of society to save, the willingness to abandon consumption today for consumption tomorrow, to accumulate capital, invest, engage in entrepreneurial activity, engage in certain types of professional activity, and shape the structure of the labor and capital markets;

4) ***institutional hypothesis***. We are talking about formal rules: laws, regulations, and the political system that determine economic behavior, in particular, the motivation to invest in physical and human capital and

innovations [15, p. 111]. As is widely recognized, the key role of formal institutions is that they form the "rules of the game" and help reduce uncertainty in socio-economic relations. It should be emphasized that we are talking about formal institutions – those based on regulatory mechanisms and instruments of state coercion. Their important feature is that, unlike geographical conditions formed millions of years ago or cultural traditions inherited from previous generations, they are mostly the result of social choice. Random factors (fluctuations), which can also affect the economic trajectory, are generally beyond control. Formal institutions, on the other hand, are subject to change and are open to influence from society. Although an individual usually cannot change the "rules of the game" on his or her own, collective action – participation in elections, shaping public opinion – creates opportunities for institutional transformation. The evolutionary nature of the (formal) institutional environment, in which society is not only an observer but also an active subject, is fundamental. This indicates that economic development can be influenced in a targeted manner through the creation or reform of existing institutions.

12.2. The role of economic security in innovation development

It should be noted that the issue of economic security as an institutional prerequisite for innovation development is rather fragmented in the scientific literature. For the most part, economic security is viewed not as a factor that forms the preconditions for innovative development, but as one of the possible consequences of such development, one of the indicators of the current state of the economic system. Many publications examine the reverse relationship – the impact of innovation and technological progress on the level of economic security. Innovative development is positioned as a tool for ensuring economic security [17], and innovative entrepreneurship is interpreted as the basis of economic security [18].

In our opinion, it is advisable to change the analytical perspective and consider the problem from the opposite side: economic security is one of the key fundamental prerequisites for the innovative development of the national economy. After all, in the absence of an adequate level of economic security, the positive impact of other development factors can be significantly offset. As soon as there is a certain degree of uncertainty about property rights or additional administrative barriers are created that impede the activities of

enterprises, any mathematically formalized models of economic growth based on production factors will give false development forecasts.

Although there are many definitions of economic security in the scientific and expert literature, it is advisable to refer first to the interpretation proposed at the official level, since it is a component of the formal institutional environment: *‘economic security is a state of the national economy that makes it possible to maintain resilience to internal and external threats, ensure high competitiveness in the global economic environment and characterizes the ability of the national economy to sustainable and balanced growth’* [19]. It is noteworthy that the legislator clearly emphasizes that economic security is a necessary condition for increasing competitiveness and ensuring sustainable economic growth.

In our opinion, the approach in which economic security is viewed as the result of the integration of both institutional hypotheses – formal and informal – with a clearly expressed security emphasis is justified, which is extremely important in the context of global turbulence, hybrid threats and conflicts (Fig. 12.1). Economic security, in this sense, contains elements of all four hypotheses mentioned earlier:

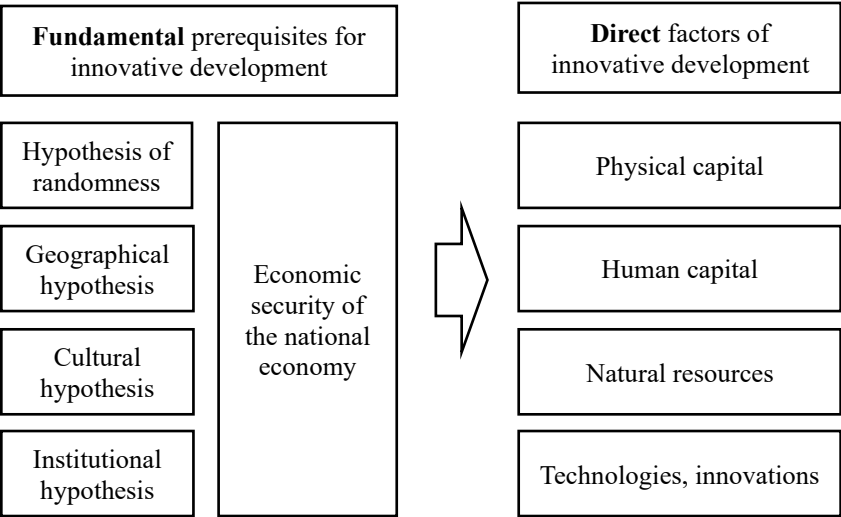


Fig. 12.1. Economic security as an institutional prerequisite for the innovative development of society

Compiled by the authors based on [15].

- the hypothesis of chance – due to the presence of factors that cannot be predicted and require effective risk management (wars, pandemics, etc.)
- geographical – due to the need to maintain resource autonomy;
- cultural – as a reflection of the behavioral reactions of economic entities to risks;
- institutional – as the ability of the state to respond effectively to threats and ensure the stability of the "rules of the game".

It is important to investigate how economic security actors create a favorable institutional environment for the innovative development of the national economy. The scientific literature presents a significant number of areas of economic security, which are classified according to different approaches and criteria. However, their complete cataloging seems excessive and has no practical feasibility within the framework of this study. Instead, it is advisable to focus on the key areas of economic security that form the prerequisites for the effective use of the main factors of economic growth – capital, labor, natural resources and technology.

A security condition for the efficient use of *capital* is stable, predictable, and cost-effective investment. For this purpose, it is necessary to ensure the existence of a number of key areas of economic security, each of which performs a specific function in strengthening institutional trust in the economy:

1) *financial security* – designed to ensure confidence in the national financial system and the sustainability of the financial infrastructure, namely: protection of the banking sector from systemic crises, insolvency and financial fraud; ensuring the stability of monetary policy, in particular the predictability of the key policy rate and inflation; effective control over public debt and budget deficit; regulation of a number of important markets, including stock, currency, insurance, etc;

2) *investment security* – this means creating a transparent, non-discriminatory and predictable institutional environment for investors: guarantees of protection of investors' rights, including foreign investors; implementation of an effective anti-corruption policy that minimizes administrative and informal pressure on investors; support for innovation and venture capital, in particular through state funds, guarantees or preferential taxation;

3) *legal security* – includes protection of property rights, including intellectual property rights; an effective and independent judicial system for economic disputes; an effective system of enforcement of court decisions;

prevention of raiding and other forms of direct and covert redistribution of assets; predictability and uniformity of the fiscal burden on business;

4) *currency and foreign economic security* aimed at reducing currency risks for investments – maintaining the stability of the national currency, developing reinvestment instruments, protecting national capital abroad, and counteracting the withdrawal of capital to offshore zones for tax evasion;

5) *innovation security* – development of the venture capital market and innovation infrastructure, expanding access to financing for high-risk technological and scientific projects, legal and economic protection of intellectual capital as an intangible asset.

In order to effectively use *human resources* as a factor of economic growth, it is necessary to create institutional and political conditions under which human capital is not only preserved but also developed, adapted to new challenges, and realized in the economy:

1) *demographic security*, the main purpose of which is to reproduce the labor potential in the economy, its quantitative and qualitative expansion. Its priority areas are to influence the dynamics of the working-age population through active demographic policy and birth rate support, reduce labor emigration, particularly among young people, facilitate immigration of highly skilled workers, and create conditions for the return of labor migrants from abroad;

2) *educational and professional security* – adaptation of the education system to the needs of the labor market, proper structuring of the post-secondary education system, effective vocational guidance for young people, support for retraining and professional development programs for adults, better adaptation of the higher education system to the real needs of business;

3) *legal security* – protection of labor rights of employees, fair labor legislation, minimization of shadow employment, effective functioning of state institutions for labor market regulation;

4) *social security* – a decent level of social protection (unemployment insurance, labor protection, affordable healthcare), development of social mobility (access to education, career development regardless of social background), prevention of social exclusion of vulnerable groups (people with disabilities, veterans, IDPs, etc.);

5) *technological and digital adaptation of the workforce* – formation of modern digital competencies necessary for functioning in the knowledge economy, facilitating the adaptation of employees to automation, IT solutions, and changes in business processes.

Efficient use of ***natural resources*** as one of the factors of economic growth involves the conservation, reproduction and rational use of the country's resource potential, taking into account environmental challenges and sustainable development goals:

1) *resource security* – rational management of natural resources (water, subsoil, forests, land, etc.) based on scientific estimates of their volumes and renewability, introduction of restrictions on excessive and inefficient use of resources, monitoring and control of the environment to prevent degradation of the resource base;

2) *energy security* – diversification of energy sources, development of renewable energy (solar, wind, bioenergy), modernization of energy infrastructure to improve energy efficiency and minimize losses;

3) *regulatory security* – clear resource legislation regulating access to subsoil, licensing procedures, production quotas, export restrictions, etc.; transparent, non-corrupt resource management system; harmonization of environmental legislation with international standards, in particular within the framework of European integration processes;

4) *food security* – preserving soil fertility, combating land degradation, supporting national food producers through technological modernization of the agricultural sector;

5) *innovative resource conservation* – introduction of environmentally friendly technologies in production, encouragement of enterprises to energy and resource efficiency, support of the circular economy, which involves the reuse of materials and minimization of waste.

The key areas of economic security that form a solid foundation for sustainable ***technological*** development are as follows:

1) *innovation security* – stimulation of R&D in the public, corporate and academic sectors, development of the innovation ecosystem (technology parks, business incubators, clusters), attraction of venture capital and creation of conditions for commercialization of innovations, protection of the results of innovation activities, including through an effective patenting system;

2) *technological security* – this refers to the sustainability and autonomy of the country's technological base in strategically important areas, namely: the formation of own strategic technological competencies (in the field of IT, defense, energy, biotechnology), reduction of critical dependence on foreign technologies, control over technology transfer, development of critical infrastructure (digital, telecommunications, energy) to support the functioning of the technological base;

3) *educational security* – priority development of technical and engineering education, training of high-tech specialists, implementation of retraining programs for workers whose professions are disappearing as a result of the spread of artificial intelligence, robotization and digitalization;

4) *legal security* – ensuring the protection of intellectual property, including copyrights, patents, and trademarks; supporting innovation through tax incentives; digitalization of public administration and administrative procedures;

5) *cybersecurity* – protection of critical information systems of the state and business, institutionalization of cyber defense (creation of responsible bodies, systems for monitoring and responding to cyber threats), and the formation of a culture of cyber hygiene in organizations and among the population.

These areas of ensuring the economic security of the national economy are of a framework nature and primarily outline the principled approaches and relevant strategic goals. This is due to the fact that each political force that forms the institutions of power in a certain period of time simultaneously offers the society its own vision of economic security, relies on a certain set of tools and offers its own "recipes" for solving certain problems related to the effective use of direct factors of economic growth. Obviously, these 'recipes' are not always verified and effective.

Formal institutions that are created in different countries can differ significantly from each other. Their specific architecture is the result of the relevant social choice, which is implemented in one form or another in a democratic social structure [20, p. 6]. It is through the electoral process, through information openness that society can in some way influence the formation of new and transformation of existing institutions – and thus the architecture of the economic security system that shapes the dynamics of economic development and growth.

Such differences in institutional structure and economic policies are commonly referred to as institutional differences. An important question arises: why do some societies create institutions that can provide a sufficient level of economic security, while others do not, and thus impede innovative development?

To explain the reasons for institutional differences, it is advisable to turn to political economy approaches and certain managerial aspects. The first key element is social conflict. Few, if any, economic changes are able to satisfy the interests of all or almost all social groups equally. Accordingly, any

institutional or political changes create winners and losers [15, p. 782]. Such conflicts have accompanied the entire history of technological progress. A well-known example is the Luddite movement in nineteenth-century Britain, when workers destroyed machines that replaced manual labor. Although from a historical perspective, technological innovations had a positive long-term effect on the economy as a whole, they became a source of losses and discontent for certain social groups.

A similar logic applies to the process of forming an institutional environment aimed at ensuring the economic security of the state. Any reform, even if it increases the overall level of economic security, inevitably changes the distribution of resources, benefits and access to power, which leads to resistance from certain social groups. For example, the introduction of electronic declaration in Ukraine caused resistance from some civil servants; the introduction of mandatory cash registers for individual entrepreneurs was accompanied by protests from small businesses, etc. Therefore, economic security is not only a static state of the economic system, but also a dynamic, rather complex and controversial political and economic process that requires, among other things, the skills of effective conflict of interest management.

The second key element of political economy, which can be used to explain the inability of some societies to create effective institutions to ensure economic security, is the problem of obligations [15, p. 783]. It consists in the fact that no government can guarantee that its successors will fulfill its obligations in their management activities. Because of this, political decisions are made without guarantees of long-term consistency, which disrupts the stability of governance processes and institutions and creates social distrust in them. As a result, politicians often focus not on maximizing economic growth, but on political expediency – the impact on their public ratings, the "correct" distribution of welfare among certain individuals and groups on whom their stay in power depends. Many management decisions needed to strengthen economic security have a delayed effect but require immediate political will. That is why they are postponed or not implemented at all, which complicates the prospects, slows down and even eliminates long-term reforms.

Thus, by the system of ensuring the economic security of the national economy, we mean the integral architecture of formal and informal institutions that regulate and ensure the stable, predictable and efficient functioning of the national economy in the face of internal and external risks

and create a favorable environment for the long-term innovative development of society. Building an effective system of economic security is a complex political and economic task, the solution of which requires social dialogue between the government, business and civil society, and inclusive participation of various social groups in the reform process.

References

1. Bacon, F., Rawley, W. (1670). *New Atlantis. A work unfinished*. In: Bacon, F., Rawley, W. (eds.), *Sylva sylvarum, or, A natural history in ten centuries: Whereunto is newly added, The history natural and experimental of life and death, or of the prolongation of life*. 9th ed. William Lee. 31 p. <https://doi.org/10.1037/13885-013>
2. Kapp, E., Wolfe, L. K., Zielinski, S. (2018). *Elements of a Philosophy of Technology: On the Evolutionary History of Culture*. University of Minnesota Press. 336 p. <https://doi.org/10.5749/j.ctv7n0cpf>
3. Heidegger, M. (1977). *The Question Concerning Technology and Other Essays*. New York: Harper & Row. 182 p.
4. Hauer, T. (2017). Technological determinism and new media. *International Journal of English Literature and Social Sciences*, 2(2), 1–4.
5. Fagerberg, J., Srholec, M., Verspagen, B. (2010). The Role of Innovation in Development. *Review of Economics and Institutions*, 1(2), 1–29. <https://doi.org/10.5202/rei.v1i2.15>
6. Bijker, W. E., Hughes, T. P., Pinch, T. (1987). *The social construction of technological systems: new directions in the sociology and history of technology*. Cambridge, MA, and London: The MIT Press. 405 p. <https://doi.org/10.1017/S0025727300049516>
7. Шумпетер, Й. А. (2011). *Теорія економічного розвитку. Дослідження прибутків, капіталу, кредиту, відсотка та економічного циклу*. Київ: Вид. дім "Києво-Могилян. акад.". 244 с.
8. Solow, R. M. (1956). A Contribution to the Theory of Economic Growth. *Quarterly Journal of Economics*, 70(1), 65–94.
9. Schultz, T. (1971). *Investment in Human Capital. The Role of Education and of Research*. New York: The Free Press. 272 p.
10. Becker, G. S. (1964). *Human Capital: A Theoretical and Empirical Analysis, with Special Reference to Education*. University of Illinois at

Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship. Available at: <https://ssrn.com/abstract=1496221>

11. *The Innovation Imperative: Contributing to Productivity, Growth and Well-Being*. Paris: OECD Publishing, 2015. <https://doi.org/10.1787/9789264239814-en>

12. Ломачинська, І. А., Горняк, О. В. (2024). Роль інновацій у розвитку національної економіки в умовах сучасних трансформацій: інноваційний розвиток, інноваційний потенціал, інклюзія інновацій. *Ринкова економіка: сучасна теорія і практика управління*. Т. 23. № 2(57). С. 56–71. [https://doi.org/10.18524/2413-9998.2024.2\(57\).325341](https://doi.org/10.18524/2413-9998.2024.2(57).325341)

13. Diachenko, D. (2025). Conceptual foundations of the innovative development: theoretical aspect. *Social Development: Economic and Legal Issues*. No. 3. <https://doi.org/10.70651/3083-6018/2025.3.02>

14. North, D. C., Thomas, R. P. (1973). *The rise of the Western World: a new economic history*. Cambridge: Cambridge University Press. 171 p. <https://doi.org/10.24201/edu.v9i01.320>

15. Acemoglu, D. (2009). *Introduction to Modern Economic Growth*. Princeton: Princeton University Press. 990 p.

16. Pasichnyk, T. O. (2024). Logical and epistemological foundations of the concept of economic structures development. *Economic Innovations*, 26(2), 65–82.

17. Неустроєв, Ю. Г., Правдивець, О. М. (2021). Інноваційний розвиток як інструмент економічної безпеки. *Український журнал прикладної економіки та техніки*, 6(4), 223–229.

18. Охріменко, І. В., Вдовенко, Н. М., Овчаренко, Є. І., Гнатенко, І. А. (2021). Інновації в системі стратегічного управління безпекою національної економіки в умовах ризиків та невизначеності глобалізації. *Економіка та держава*, 8, 4–9. <https://doi.org/10.32702/2306-6806.2021.8.4>

19. Про затвердження Методичних рекомендацій щодо розрахунку рівня економічної безпеки України: Наказ від 29.10.2013 № 1277. Available at: <https://zakon.rada.gov.ua/rada/show/v1277731-13#Text>

20. Петруня, Ю. Є. (2017). Управлінські рішення та «суспільна думка»: макрорівневий аналіз. *Науковий погляд: економіка та управління*, 1, 5–11.

Chapter 13
The European Union's Common Foreign and Security Policy
(CFSP): challenges and prospects for Ukraine
(N. Shpak)

The Common Foreign and Security Policy (CFSP) of the European Union (EU) is one of the key components of the European security architecture in the 21st century. The CFSP aims to ensure the security of the EU Member States, strengthen international stability, and promote democratic values and the rule of law on the international stage. In the context of Russia's full-scale armed aggression against Ukraine and further geopolitical changes in Europe, the CFSP is gaining key importance as an instrument for ensuring security and stability on the continent.

The CFSP is the European Union's strategy to ensure peace, stability, and security in its Member States and beyond. The CFSP focuses on the following principles: promoting international cooperation; preserving democratic values; and preventing conflicts worldwide.

Key policy objectives include: strengthening the EU's role in global diplomacy; addressing global challenges such as terrorism, cyber threats, and migration; and supporting international peacekeeping missions.

Simultaneously, the challenge is not only to increase spending, but also to invest wisely and collectively. European security must be underpinned by credible capabilities, institutional readiness, and political cohesion. Until then, Europe will remain on the periphery of global negotiations, even when the stakes are highest on its own soil [1]. EU countries have backed a proposal to create a €150 billion (\$168.3 billion) fund to strengthen Europe's defenses, known as the Security for Europe (SAFE) Program [2].

The plan, proposed by the European Commission, would be financed by joint borrowing and would provide loans to EU members and some other countries, such as Ukraine, for projects that strengthen their defenses and develop the European defense industry [3].

The EU and its Member States are increasing their defence spending and investment in a period of a radically changed security environment. In 2024, the defence spending of Member States reached €343 billion, of which €106 billion was allocated to investment. In 2025, it will reach around €381 billion [4]. The EU complements and reinforces the individual efforts of Member States by supporting increased national defence spending, utilizing EU budgetary resources, and promoting private investment in the defence sector. The increase in defence spending represents a 19% increase in Member States' defence spending between 2023 and 2024. The institutional framework ensuring Ukraine's participation in the Common Foreign and Security Policy and the Common Security and Defence Policy (CSDP) (CFSP) is in place. Ukraine's compliance rate with the CFSP (High Representative's declarations on behalf of the EU and Council decisions on sanctions) in 2023 was 89%. As of 30 September 2024, the compliance rate had increased to 95%. This demonstrates a clear political intention to align with the CFSP [4].

Ukraine continues to align its actions with the EU's restrictive measures. Ukraine has mechanisms in place to ensure the effective implementation of EU sanctions.

Secretary General Alain Berset: 'We must never forget that democracy is our first line of defence. Europe needs a reboot: A New Democratic Pact for Europe. Because what is at stake is Europe's security, the values we share, and our place in the world' [6].

The Secretary General's annual report assesses the state of democracy, human rights, and the rule of law in the 46 member states of the Council of Europe over the

two years since the publication of the last full report in 2023.

Of particular note is Chapter 31 ‘Common Foreign, Security and Defence Policy (CFSP/CSDP)’ of Cluster 6 of the EU accession negotiations, which covers the alignment of the candidate country’s foreign policy with the European Union, including positions in international organisations, diplomatic initiatives, and security mechanisms. The chapter also covers the implementation of joint decisions of the Council of the EU, in particular on sanctions regimes, Common Security and Defence Policy (CSDP), crisis response, and peacekeeping operations [4].

The EU’s Common Foreign and Security Policy (CFSP) is a key instrument for ensuring peace, stability, and security in the face of geopolitical changes caused by Russia’s full-scale war against Ukraine. The policy aims to strengthen Europe’s defence capabilities through collective investments that complement the growth of national defence spending. Ukraine is actively aligning its policies with the CFSP, having achieved 95% compliance with EU sanctions decisions in 2024, demonstrating its clear political intention to integrate into the European security space [4].

The above indicates that cluster 6 of the EU accession negotiation process is an indicator of foreign policy solidarity and strategic compatibility with the EU, which is of critical importance for the EU accession process, especially in the context of the new security situation in Europe after the Russian aggression against Ukraine.

13.1. Stages of CFSP development

The EU's Common Foreign and Security Policy has evolved from intergovernmental cooperation to a more integrated decision-making system.

Since the signing of the relevant treaties (Table 13.1), the CFSP has gone through several stages of development.

Table 13.1

Stages of development of the CFSP

Title of the agreement	Year of signing	Contents
Maastricht Treaty [6]	1993	The creation of the European Union (EU) as a political and economic union, comprising the three main pillars of the EU: the European Communities, the Common Foreign and Security Policy, and cooperation in the field of justice and home affairs.
Treaty of Amsterdam [6, *consolidated version 1997]	1999	Creation of the position of High Representative of the EU for Foreign Affairs and Security Policy.
Treaty of Nice [6, *consolidated version 2002]	2001	Consolidation of intergovernmental cooperation in foreign policy.
Lisbon Treaty [7]	2009	Strengthening the role of the High Representative, establishing the European External Action Service (EEAS), and implementing the Permanent Structured Cooperation (PESCO) mechanism. Strengthening solidarity between the Member States of the European Union (EU) in combating external threats in the context of mutual defence.

In light of Russian aggression against Ukraine, the CFSP plays an important role in supporting Ukrainian statehood and strengthening security in the region.

Russia's war against Ukraine concerns not only the freedom and existence of Ukraine as a whole, but also the concrete future of Europe's hardline security policy. Russia is trying to replace the cooperative and democratic security order in Europe, the principles of which were set out 50 years ago in the Helsinki Final Act [8], one where the strong begets the right, and Russia is an empire that dominates large areas of Europe, which would pose an existential threat to the security of the EU and its member states.

A striking example of the competing narratives between the EU and Russia is Ukraine's pursuit of Euro-Atlantic integration while simultaneously containing Russian military aggression since the annexation of Crimea in 2014 and the occupation of Luhansk and parts of the Donetsk regions. The ongoing full-scale invasion that began in 2022 is, in this case, not only a backdrop but also a battlefield for the struggle for Ukrainian identity.

The EU's decision to open accession negotiations with Ukraine and Moldova is a geostrategic investment [9], which can strengthen the European security order and prevent Russia from achieving its ambitions. It does so not only by defending the sovereign right of Ukraine and Moldova to the European path, but also by providing military capabilities and strategic resources for the EU. However, while Ukraine and Moldova can contribute to the EU's security in the long term as full members, it is Europe that must first and foremost ensure their security.

In a scenario where a settlement or ceasefire is reached in Russia's war against Ukraine, the EU could – given its obligations to Ukraine through the EU accession process, as well as US pressure on Europe to take care of its own security – find itself drawn into Ukraine's security. Ensuring Ukraine's long-term hard security (achieving peace) would require the EU to move away from the status quo and break old taboos. However, such a tectonic shift may be feasible, given the forces at work in the current geopolitical environment.

The EU has shown in the past that major external events, such as German reunification, the 2008 financial crisis, and the COVID-19 pandemic, can make the impossible possible. The development of European cooperation is driven not so much by political vision as by necessity. For example, if US President Donald Trump were to demand that Europe take care of Ukraine's security as a precondition for the continuation of US security guarantees to NATO, the EU could be forced to undertake painful reassessments. There is therefore reason to take a closer look at the steps that European policymakers could take to provide Ukraine with reliable security guarantees and to ensure the hard security of the EU's eastward enlargement.

Ukraine is making significant progress in aligning with the EU's Common Foreign, Security and Defence Policy (CFSP/CSDP), having achieved 95% compliance with EU decisions and declarations as of September 2024 [4]. This indicates a clear political course towards integration into the European security space, active involvement in joint initiatives, and the formation of institutional capacity (Table 13.2).

The EU statement on the launch of accession negotiations with Ukraine and Moldova in 2024 describes enlargement as a geostrategic investment. It is worth highlighting four security-related reasons why this is so. First, a scenario in which Ukraine is forced to abandon its ambitions for full integration with the EU, and its sovereignty is thus limited, would mean that Russia is allowed to benefit from its aggression and nuclear blackmail.

Table 13.2

Correlation between the requirements and the current state of Ukraine in the field of EU Foreign and Security Policy – (CFSP/CSDP)

EU requirements (cluster 6)	Current status: the case of Ukraine
Coordination of foreign policy with the EU (statements, declarations, positions in international organizations)	Ukraine's CFSP compliance rate increased from 89% in 2023 to 95% as of September 2024 – demonstrating a high level of political alignment [4].
Enforcement of restrictive measures (sanctions)	Ukraine has established mechanisms for implementing EU sanctions and regularly updates them in accordance with EU Council decisions [16].
Participation in the Common Security and Defense Policy (CSDP) – peacekeeping missions, crisis response	Ukraine is already involved in individual CSDP projects and has expressed its readiness for greater participation in joint EU defense and security initiatives [2].
Institutional capacity to coordinate CFSP/CSDP	An institutional framework for coordination of actions is functioning; the Ministry of Foreign Affairs of Ukraine coordinates policy within the CFSP framework [4].
Defense cooperation and access to European programs	Ukraine is included in the Security for Europe Program (SAFE, 150 billion euros) and is also actively integrating into the European defense industry [2].

This also applies to Moldova, which confirmed its ambitions for EU membership in a national referendum against the backdrop of Russia's intense hybrid warfare. Disrespect for the sovereign right of Ukraine and Moldova to follow a European path paves the way for a security order divided into spheres of interest, where competition for territory, resources, and influence is resolved by force. Such an order would pose an existential threat to the sovereignty and territorial integrity of smaller countries and undermine the principles of the European security order set out in the Helsinki Final Act of 1975 [8], including respect for national sovereignty and territorial integrity of states, the prohibition of the use or threat of force, and the fulfillment of obligations under international law. Successful outcomes of the EU accession processes of Ukraine and Moldova would prevent such developments, thereby strengthening the European security order and international law.

Secondly, if Ukraine and Moldova remain in the grey zone between the EU/NATO and Russia, this will entail significant risks for the security of the whole of Europe, as Russia will be able to use these countries as arenas for the continuation of its conventional and hybrid acts of aggression. In particular, a delayed or unsuccessful enlargement of the EU would allow

geopolitical actors other than Russia, not least China, to increase their influence in the region. In the current geopolitical situation, characterized by interstate tensions, rivalries, and instability, there is no status quo ante to which one can return: either the EU exports stability to the East or imports instability from the East.

Third, Ukraine has one of the largest, strongest, and most experienced regular armies in Europe, and its officers and soldiers have direct combat experience in a war against an aggressor in Europe. Ukraine has experience in areas such as demining, reconnaissance, and counter-drones. Both Ukraine and Moldova have experience in countering and countering Russian cyber-attacks and disinformation campaigns. Both candidate countries could thus contribute to a common EU military system.

Delays caused by unanimity risk undermining the EU's crisis response and global influence.

Russia's full-scale invasion of Ukraine has highlighted the urgent need for rapid decision-making [10].

Arguments in favour of qualified majority voting: Adopting a more effective qualified majority voting system would significantly strengthen the EU's geopolitical influence. This approach would allow the EU to act decisively and gain authority in world affairs, improving its ability to shape international norms and respond quickly to challenges [11].

A qualified majority can create more opportunities for increased cooperation and cohesion within the EU [12]. Moreover, it already exists – after Brexit, 85% of all decisions were approved by consensus [11].

The emerging consensus within the EU's supranational bodies (the European Commission) as well as the Member States has the support of Member States such as Germany and France, it has the gradual support of other Member States: the Friends Group on qualified majority voting, in particular in the Common Foreign and Security Policy (France, Spain, Germany, Italy, Luxembourg, the Netherlands, Slovenia, Italy, Belgium, Denmark, Romania, Sweden).

The persistent difficulties in reaching consensus may threaten the EU's ability to uphold its fundamental values, as stated in Article 2 of the Treaty on European Union [6] the argument in favour of qualified majority voting – the existing legal mechanisms confirm that the introduction of qualified majority voting is both feasible and fully consistent with the EU legal framework, which enhances stability and security within the Union 'The

Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights...' [6].

Transitional provisions ('bridging clauses') are mechanisms that allow for adjustments to decision-making procedures or for the extension of institutional powers in certain areas.

Treaty of Lisbon (2007) [7] introduced: specific transitional provisions clearly designed for application, in particular within the CFSP, a qualified majority minimizes the risk of external influence and veto by individual states. In particular, Hungary demanded concessions during the vote on sanctions against Russia [13].

European Parliament [14] proposed a treaty change to move to qualified majority voting in the areas of restrictive measures.

The Common Foreign and Security Policy (CFSP) has a special status in the EU legal architecture, of which the unanimity rule in the Council is part. The report [15] possible alternatives to CFSP decisions taken based on unanimity, such as moving to qualified majority voting (QMVO), are analysed, including their costs and benefits.

The study develops several policy options, including current legal options, options requiring treaty change, and options requiring the abandonment of intergovernmental governance in the CFSP.

The current unanimity rule hinders timely and effective decision-making. Article 24 of the Treaty on European Union (TEU) [6] states that decisions under the Common Foreign and Security Policy (CFSP) are normally taken by unanimity, except where the Treaties provide otherwise. However, this rule has led to delays and policy paralysis, particularly in emergencies.

Article 24(1) of the Treaty on European Union [6] states: 'The CFSP shall be defined and implemented by the European Council, acting unanimously, except where otherwise provided for in the Treaties'.

The transition from unanimity to qualified majority voting (QMVO) in selected areas of the Common Foreign and Security Policy is often portrayed as a panacea for a more effective EU international actor. This would change the dynamics of negotiations and avoid veto blocking, while still preserving the integrity of the EU and allowing for its implementation. Regarding the introduction of qualified majority voting, the caveat of Article 31(2) of the TEU [6] extends to all areas where qualified majority voting is used.

EU sanctions policy against Russia weakens the aggressor's economic capabilities [17]. Infographics [20] demonstrates the significant impact of

sanctions on the Russian economy, which deters further escalation of the conflict.

The EU provides significant material and financial assistance to Ukraine aimed at strengthening its defense capabilities. The opening of negotiations on Ukraine's accession to the EU is an important geostrategic step that strengthens European security and prevents Russia's ambitions to revise the European security order.

13.2. CFSP challenges and prospects

Despite significant achievements, the CFSP faces a number of challenges. Consensus in decision-making – the need for unanimity in foreign policy matters often hampers the EU's responsiveness. When voting on foreign and security policy issues in the Council of the EU, requests for changes from society should be used, rather than from the European Parliament, for qualified majority voting.

Citizens support wider use of qualified majority voting in foreign policy to ensure faster and more effective EU action [18]. Support for qualified majority voting in foreign and security policy from the wider public. Public support for a stronger and more united EU foreign policy is growing. Surveys conducted during the Conference on the Future of Europe [18], show that a large majority of EU citizens are in favour of reducing the use of the veto right in the Council to ensure more efficient decision-making. Citizens expressed frustration with the EU's inability to act quickly on critical issues due to internal disagreements.

European Eurobarometer data [18] indicate:

- 77% of Europeans support a common security policy between EU countries;

- 69% of EU citizens are in favour of a common foreign policy between Member States.

The EU needs to improve its decision-making capacity, particularly in the Common Foreign and Security Policy (CFSP), speaking with one voice and acting as a truly global player, projecting a positive role in the world and a transformative response to any crisis, in particular, in the area of the CFSP, issues that are currently decided unanimously, which should normally be changed, should normally be decided by qualified majority [14].

In a resolution in June 2022, the European Parliament proposed a treaty change to move to qualified majority voting in areas of restrictive measures [14].

Request for changes from the European Parliamentary Research Service (EPRS). EPRS has clearly called for changes to the decision-making procedures in the CFSP, recommending a move from unanimity to qualified majority. EPRS argues that the current unanimity rule imposes a “high price of not being European”, preventing the EU from taking swift and unified action in response to new geopolitical threats [15].

Underfunded – EU member states’ defense budgets, although growing (expected to be €284 billion in 2025) [19], still inferior to the US and China.

Hybrid threats and cybersecurity require increased coordination between member states.

The following steps are proposed to overcome these challenges:

1. The transition to qualified majority voting in the CFSP will allow for faster and more efficient decision-making.
2. The integration of Ukraine and Moldova into CFSP forums and their involvement in the decision-making process will strengthen European security.
3. Strengthening cooperation with NATO - forming a strategic partnership for a joint response to threats.
4. Investment in defense infrastructure - joint financing through defense bonds.
5. Information campaign to raise awareness among EU citizens about the importance of eastern enlargement for European security.

The EU's common foreign and security policy is a key instrument for strengthening European security in the face of modern geopolitical challenges. The policy plays an important role in supporting Ukraine in its resistance to Russian aggression and contributes to strengthening stability in the region. Further improving decision-making mechanisms, enhancing cooperation with NATO, and involving Ukraine in CFSP processes will help the EU respond more effectively to security challenges and ensure peace and stability in Europe.

The geopolitical theatres of events in Ukraine, the Middle East, the South China Sea and the Indo-Pacific region are increasingly interconnected, as Russia and China, in particular, deepen their ties, and pose significant challenges to global peace and security, as well as to the rules-based international order, which the international community must address;

Stresses the increasing number of attacks and hybrid threats aimed at undermining democratic values and structures, including during elections, as well as the unity and commitment of citizens to European societies based on values and the rule of law; believes that this trend is a paradigm shift, as it changes the logic of building international security based on respect for international law, a rules-based global order, and multilateralism [4].

The defense budgets of EU member states are approximately 250 billion US dollars (236 billion euros), and will be 284 billion euros in 2025 [19].

The European Union (EU) has imposed a series of sanctions against Russia in response to its aggression against Ukraine [20]. The sanctions include economic restrictions, asset freezes, and entry bans for individuals and entities.

Besides, the European External Action Service has published an infographic [20], which illustrates the impact of EU sanctions on Russia in response to its aggression against Ukraine.

NATO countries consider including contributions to Ukraine's defense in new earmarked spending [19].

The declaration stipulates that the Alliance members will spend at least 5% of GDP on defense: 3.5% on basic needs, another 1.5% on infrastructure, cybersecurity, and training of the population.

The declaration does not mention Ukraine's accession to NATO or the promise of \$40 billion in aid, as last year. Russia is recognized as a threat, but is not called an aggressor, and China is not mentioned in the document.

The transition from the principle of unanimity to qualified majority in decision-making within the framework of the CFSP may become key in the context of increasing the efficiency and effectiveness of the EU's Common Foreign and Security Policy. Such an approach will avoid blockages by individual states, strengthen the geopolitical weight of the Union, and create conditions for greater unity in countering external threats. For Ukraine, this will mean faster adaptation to common EU decisions and increased integration into the European security space, which meets its strategic interests and will contribute to greater resilience of Europe in the face of challenges.

Conclusions

Cluster 6 of the EU accession negotiation process is an indicator of foreign policy solidarity and strategic compatibility with the EU, which is of critical importance for the EU accession process, especially in the context of

the current security situation in Europe after the Russian aggression against Ukraine. The EU provides significant material and financial assistance to Ukraine aimed at strengthening its defense capabilities. The opening of Ukraine's accession negotiations to the EU is an important geostrategic step that strengthens European security and prevents Russia's ambitions to revise the European security order.

The transition from the principle of unanimity to qualified majority in decision-making within the CFSP framework could be key in the context of increasing the effectiveness and efficiency of the EU's Common Foreign and Security Policy. Such an approach would avoid blocking individual states, strengthen the geopolitical weight of the Union and create conditions for greater unity in countering external threats. For Ukraine, this will mean faster adaptation to the EU's common decisions and enhanced integration into the European security space, which meets its strategic interests and will contribute to Europe's greater resilience to challenges.

The European Union's Common Foreign and Security Policy (CFSP) is emerging as one of the key instruments for shaping a new security order in the face of global threats and Russian aggression against Ukraine. Ukraine has demonstrated a high level of political compatibility with the EU, having achieved unprecedented compliance with the CFSP, and is gradually integrating into common security and defense mechanisms. The challenges facing the CFSP – the need to reform the decision-making process, strengthen financing, and combat hybrid threats – at the same time open up prospects for deepening cooperation between Ukraine and the EU. For Europe, Ukraine's accession is of not only political but also strategic importance, as it strengthens the continent's defense capabilities and strengthens the international agenda based on the rule of law.

References

1. Gamkrelidze, T. (2025). *Europe at a crossroads: strategic security dependency in the age of uncertainty*. Available at: <https://neweasterneurope.eu/2025/05/05/europe-at-a-crossroads-strategic-security-dependency-in-the-age-of-uncertainty/>
2. European Commission. (2025). *Council Regulation establishing the Security Action for Europe (SAFE) through the reinforcement of European defence industry Instrument* (COM(2025) 122 final). Brussels. Available at: https://defence-industry-space.ec.europa.eu/document/download/6d6f889c-e58d-4caa-8f3b-8b93154fe206_en?filename=SAFE%20Regulation.pdf

3. European Council. (2025). *Security and defence*. Council of the European Union. Available at: <https://www.consilium.europa.eu/en/topics/security-and-defence/>
4. European Commission. (2024). *Communication on EU enlargement policy – annual report*. Available at: https://enlargement.ec.europa.eu/ukraine-report-2024_en (accessed 13 September 2025).
5. Council of Europe. (2025). *Towards a New Democratic Pact for Europe. Report of the Secretary General*. Available at: <https://rm.coe.int/2025-report-of-the-secretary-general-of-the-council-of-europe-en-final/1680b5ad96>
6. European Parliament (1992). *Treaty on European Union*. Document 11992M/TXT. Available at: <http://data.europa.eu/eli/treaty/teu/sign> (accessed 10 September 2025). 10 (consolidated version 1997). 11 (consolidated version 2002).
7. European Parliament. (2007). *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community* (Document 12007L/TXT). Available at: <http://data.europa.eu/eli/treaty/lis/sign>
8. Organization for Security and Co-operation in Europe (OSCE). (1975). *Conference on Security and Co-Operation in Europe Final Act, Helsinki*. Lausanne: Imprimeries Réunies S.A. Available at: https://www.osce.org/files/f/documents/5/c/39501_1.pdf
9. Emerson, M., Blockmans, S. (2022). *From Geopolitics to Enlargement: Rethinking the Eastern Partnership*. CEPS Policy Brief, No. 2022-20. Available at: https://cdn.ceps.eu/wp-content/uploads/2022/06/CEPS-PI2022-20_New-Agenda-for-EU-Enlargement.pdf
10. European Parliamentary Research Service (EPRS). (2021). *Qualified Majority Voting in Foreign and Security Policy: Pros and Cons*. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)659451](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)659451)
11. European Commission (2018). *Qualified Majority Voting: A Tool to Make Europe's Foreign and Security Policy More Effective*. Available at: https://commission.europa.eu/system/files/2018-09/soteu2018-factsheet-qmv_en.pdf

12. Communication from the Commission to the European Council, the European Parliament and the Council (2018). *A Stronger Global Actor: A More Efficient Decision-Making for EU Common Foreign and Security Policy*. Available at:

<https://www.statewatch.org/media/documents/news/2018/sep/eu-com-cfsp-gmv-proposals-communication-com-18-647.pdf>

13. Hollander, S. (2024). *Audience question: What to do with the EU veto?* Clingendael. Available at:

<https://www.clingendael.org/news/audience-question-what-do-eu>

14. European Parliament (2022). *European Parliament Resolution of 9 June 2022*. Available at:

https://www.europarl.europa.eu/doceo/document/TA-9-2022-0244_EN.html

15. Dr Navarra, C. and others. (2023). *Qualified majority voting in EU common foreign and security policy*. European Parliamentary Research Service, Brussels. Available at:

[https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740243/EPRS_STU\(2023\)740243_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740243/EPRS_STU(2023)740243_EN.pdf)

16. Про синхронізацію санкційного тиску України, Європейського Союзу та інших учасників Групи семи на Російську Федерацію і пов'язаних з нею суб'єктів. Рішення Ради національної безпеки і оборони України від 27 червня 2025 року. Available at: <https://www.president.gov.ua/documents/4222025-55429>

17. European Council / Council of the European Union. (2025). *EU sanctions against Russia*. Available at: <https://www.consilium.europa.eu/en/policies/sanctions-against-russia/>

18. European data. Standard Eurobarometer STD101. (2024). Directorate-General for Communication. Available at: https://data.europa.eu/data/datasets/s3216_101_3_std101_eng?locale=en

19. Statista Research Department. (2025). *Defense expenditures of NATO member states as a share of GDP 2025*. Available at: <https://www.statista.com/statistics/584088/defense-expenditures-of-nato-countries/#statisticContainer>

20. European Commission. (2023). Directorate-General for Communication, *EU sanctions against Russia following the invasion of Ukraine*, Publications Office of the European Union. Available at: <https://data.europa.eu/doi/10.2775/127745>

Chapter 14

Formation of a regional policy of public administration cohesion with due regard to EU regulations: adaptation to security challenges and post-war recovery (V. Vorotin, N. Vorotina, V. Prodanyk)

Martial law has generated a special and unique model of governance at the state and regional levels in Ukraine. This experience will become an important component in applying a distinctly Ukrainian management model during martial law and in addressing issues related to the state's independence. The transformations that have recently taken place in the national economy are accompanied by significant institutional changes in the system - its mechanisms and instruments - of public governance and administration, particularly in terms of shaping a strategic vision for further development and the restoration of state-building based on the principles of European cohesion policy and safety of vital activity.

During this challenging period, a negative trend can be observed: the growing aggressive influence of external threats (Russia's war against Ukraine) on Ukraine's public governance system, particularly on the effectiveness of organizational and legal mechanisms for ensuring economic resources, which were practically not adapted to the conditions of martial law and therefore required urgent regulatory adjustments and refinement. This work is being carried out by the Verkhovna Rada of Ukraine around the clock [1].

It should be noted that the risks and threats to the entire governance system - and to economic (resource and reserve) security in particular - draw attention to the need to evaluate vulnerable components of the mechanisms and instruments of the public (state and local) governance system under martial law. In our view,

such components include: significant structural imbalances; monopolization and lack of transparency in certain sectors; barriers to the development of the military and defense industries; insufficient attention to civil protection of the population and territories; unresolved energy and technological dependence on Russia; uncontrolled outflow of material and financial resources from Ukraine; the operations of shadow structures; the presence of hostile Russian agents; the absence of a professional school of public administration; and other vulnerabilities [2].

The further development of mature market relations in national economic practice - with strong regions and subregions - is a strategic direction for the decentralized system of public governance and administration after Victory. Within this system, the role of a cohesive national and regional development policy (section 14.1) not only does not diminish under current conditions of reforming the entire governance and security system but, on the contrary, grows, acquiring new quality and effectiveness amid real threats to the state's existence. This chapter also examines the economic and administrative foundations of balanced development in the context of European integration processes in Ukraine (section 14.2), and outlines the mechanisms of public governance of state reserves of material assets (section 14.3).

14.1. Cohesion policy as an object of public governance in Ukraine: EU regulations

The Cohesion Policy of the European Union is one of the key strategies of integration-oriented development aimed at reducing territorial, economic, and social disparities among regions, strengthening internal unity, and creating the preconditions for sustainable growth of the state and its regions. For Ukraine - currently experiencing war, preparing for post-war recovery, and simultaneously advancing along the path of European integration – the development of its own cohesion policy, aligned with EU regulations and

practices, becomes a critically important task. This involves not the mechanical transfer of European instruments but the adaptation of values, principles, and methods to the specific conditions of a state that is simultaneously rebuilding from destruction and facing ongoing security challenges [3].

The principles of effective functioning of organizational components of public governance, and of the interaction between managerial relations and the economic system as a whole, occupy a central place in the works of many scholars. Significant contributions have been made by foreign researchers such as M. Albert, R. Ackoff, D. Woodward, J. Grayson, P. Drucker, R. Dornbusch, B. Karloff, E. Mayo, Ph. Kotler, A. Maslow, M. Mescon, W. Ouchi, M. Porter, H. Simon, F. Taylor, R. Falmer, H. Ford, S. Fischer, Ph. Hedaouri, L. Iacocca, among others.

Theoretical and methodological foundations of public governance, as well as mechanisms for shaping and implementing state policy across various spheres of public life, are explored in the works of M. Bilynska, L. Vorotina, K. Vashchenko, A. Zadoia, V. Kuibida, M. Kravchenko, O. Petroie, O. Pukhkalov, S. Romaniuk, H. Riabtsev, S. Serohin, I. Surai, O. Sukhodolia, V. Troshchynskyi, S. Fedulova, S. Khadzhyradieva, and others.

Ukrainian scholars - including B. Averyanov, O. Amosov, O. Andriiko, V. Bakumenko, Yu. Bytiak, L. Voronova, S. Dubenko, Yu. Kuts, Yu. Pakhomov, N. Plakhotniuk, L. Prykhodchenko, A. Selivanov, O. Sushynskyi, V. Shapoval, Yu. Shemshuchenko, A. Chukhno, and others - have dedicated their research to the specifics of the functioning of this social phenomenon in Ukraine and its impact on the democratization of public administration. However, to date, there is a lack of systematic studies concerning the strategic vision of European state-building and the reserve component of cohesion within Ukraine's public governance system, particularly in the period following Victory over the Russian Federation.

Cohesion in public governance is a multidimensional scientific category. It encompasses the integration of different levels of government - central, regional, and local - into a unified system of goals and priorities; the coordination of resources across the state, business, and civil society; and ensuring equitable access to development opportunities for all territories and social groups. In the post-war context, this policy should become a key instrument not only for rebuilding infrastructure but also for strengthening social resilience, reintegrating affected communities, and forming new models of regional development aligned with EU standards.

EU regulations that define the framework of cohesion policy are based on the principles of programming, partnership, multi-level governance, and subsidiarity. For Ukraine, an urgent task is to integrate these principles into its national system of public (regional and local) governance, where policy fragmentation, weak coordination among public authorities, and regional disparities remain significant challenges. Adaptation to European standards implies that, in the course of recovery, Ukraine must develop transparent rules for the functioning of public governance, strategic planning, and monitoring the use of resources and reserves, as well as ensure public participation in decision-making processes.

The planning cycle up to 2027 includes five key EU provisions concerning Cohesion Policy. All of them are aimed at providing institutional support to EU Member States, in particular:

1. Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund, and the European Maritime, Fisheries and Aquaculture Fund, and financial rules for those funds as well as for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy.

2. Regulation (EU) 2021/1059 of the European Parliament and of the Council of 24 June 2021 on specific provisions for the European territorial cooperation goal (Interreg) supported by the European Regional Development Fund and external financing instruments.

3. Regulation (EU) 2021/1058 of the European Parliament and of the Council of 24 June 2021 on the European Regional Development Fund and the Cohesion Fund.

4. Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+) and repealing Regulation (EU) No 1296/2013.

5. Regulation (EU) 2021/1056 of the European Parliament and of the Council of 24 June 2021 establishing the Just Transition Fund.

A. Tkachuk and his colleagues from the Institute for Civil Society have thoroughly and promptly prepared and published an unofficial translation of Regulation (EU) 2021/1056. The European Union has created the new Just Transition Fund to support the population, economy, and environment of territories experiencing significant environmental, economic, and social

challenges related to the transition toward the EU's energy and climate objectives by 2030 [4].

Thus, cohesion policy emerges not only as a technical tool of regional development but as a strategic component of state reconstruction, enabling the alignment of security needs, economic growth, and societal integration. Its successful implementation is a prerequisite for Ukraine's sustainable renewal and its gradual integration into the European space.

Cohesion policy takes a special place within the system of public governance in contemporary European states. It is shaped as a response to structural imbalances of development and challenges of socio-economic inequality, while simultaneously acquiring a strategic dimension in the context of security, integration, and the resilience of societal systems. For Ukraine - facing full-scale aggression and post-war recovery – cohesion in public governance becomes not only an objective of integration policy but also one of the key mechanisms of survival and progressive development.

In EU regulations, cohesion policy is defined as a targeted activity aimed at reducing territorial disparities, strengthening regional competitiveness, ensuring social justice, and creating conditions for economic growth that is balanced across space. The main instruments for its implementation are the EU's structural and investment funds, which accumulate substantial financial resources and channel them to support regions with lower levels of development. At the same time, cohesion policy involves not only financial distribution but also the establishment of institutional mechanisms for partnership, programming, multi-level governance, and democratic participation of communities.

Particular attention should be given to the issue of security as an integral component of regional cohesion policy. European practice demonstrates that security considerations are incorporated into cohesion policy through investments in infrastructure, digitalization of governance, development of social capital, and strengthening the institutional capacity of communities. For Ukraine, however, this dimension must be expanded to include military and security-related factors, such as the formation of resilient civil protection systems, the creation of reserve infrastructural capacities, support for internally displaced persons, and the restoration of communities in frontline regions.

In the long-term perspective, cohesion policy should become a foundation for Ukraine's integration into the European space. It creates the prerequisites for harmonizing the public governance system with EU

principles, which will ensure not only access to financial instruments but will also increase trust in Ukrainian institutions from both citizens and international partners. Through cohesion, it becomes possible to combine recovery processes with the modernization of the state, ensure the fair distribution of resources, prevent social conflicts, and lay the groundwork for sustainable development in the post-war period.

Thus, cohesion policy in public governance is not merely an adaptation to European regulations but a profound transformation of Ukraine's development model. It is intended to unite society around the values of security, equality, and solidarity, to create institutional foundations for recovery, and to ensure gradual integration into the European space on the basis of resilience, mutual trust, and innovative approaches to regional governance.

The security dimension of cohesion acquires particular significance in post-war conditions. In Ukraine, regional cohesion policy cannot be implemented without taking into account the need to create safe living conditions for citizens, protect critical infrastructure, and ensure energy and food security. Regional cohesion in this paradigm is not only about reducing socio-economic disparities but also about strengthening the ability of regions to adapt, survive, and develop amid prolonged crises. This approach allows cohesion to be viewed as an instrument for building national resilience, based on the integration of resources of the state, business, civil society, and international partners.

Thus, the theoretical and methodological foundations of regional cohesion policy in public governance in Ukraine are being formed at the intersection of European practices and national challenges. On the one hand, they must rely on tested EU principles – programming, subsidiarity, partnership, and multi-level governance; on the other hand, they must reflect the specifics of wartime experience, the needs of post-war recovery, and the strategic objective of European integration. Such a policy can ensure not only the economic leveling of regions but also the consolidation of society, the restoration of trust in the state, and the formation of a coherent national space that is resilient to future challenges.

14.2. Economic and managerial foundations of balanced development in the context of Ukraine's European integration processes

Balanced development under current European integration processes is one of the key priorities of Ukraine's public policy, as it combines economic growth, social equity, environmental sustainability, and the institutional capacity of the state. This issue becomes particularly relevant in the context of post-war recovery, when the country faces extensive infrastructure destruction, a decline in production capacity, socio-economic disparities, and an increasing need to modernize management practices.

The academic literature emphasizes that balanced development is impossible without the integration of economic and managerial mechanisms. The economic dimension includes strategic investment planning, production modernization, development of innovative economic sectors, support for small and medium-sized enterprises, and the introduction of green and digital economy approaches. The managerial aspect consists in establishing an effective system of public governance capable of ensuring policy coordination, transparency and accountability, resource mobilization, and the participation of civil society [5].

In the context of European integration, it is particularly important to align national strategies with international standards, which ensures access to EU financial instruments, strengthens the legitimacy of reforms, and promotes Ukraine's integration into the European political and economic space. The scientific approach to studying these processes is grounded in the concepts of resilience, transformative governance, and participatory governance, which provide complexity, flexibility, and effectiveness in recovery.

Thus, the economic and managerial foundations of balanced development form the basis for Ukraine's strategic recovery, determine modernization priorities, and lay the groundwork for long-term resilience, integration, and strengthened statehood. A scholarly analysis of this combination makes it possible to identify key success factors and directions for implementing state policy in the areas of recovery and European integration.

Balanced development is a key factor for the stability and resilience of any country's economy. In the context of European integration, Ukraine must strive to align its economic practices with the requirements of the European Union. Balanced development involves the effective use of natural, human,

and financial resources to ensure sustainable economic growth, improve citizens' quality of life, and address social and economic inequalities between regions.

The European Union has a well-developed infrastructure for supporting balanced regional development through the use of structural and investment funds, particularly the European regional development fund (ERDF) and the European social fund (ESF). These funds support regions facing economic hardship by providing opportunities to develop infrastructure, create jobs, and improve living standards.

It should be noted that solidarity, sustainable development, and inclusiveness are fundamental principles of the EU's economic development. This means that resources must be distributed in a way that ensures equal opportunities for all countries and regions, including those facing substantial development challenges or located on the European periphery. These principles are particularly important for Ukraine as it adapts to European standards, especially in the areas of post-war recovery and integration into the single European economic space.

At the same time, the European Union applies a comparative approach to the development of individual regions, which makes it possible not only to compare economic indicators but also to consider social, environmental, and cultural dimensions. This ensures a more flexible adaptation to the specific needs of each region - an important factor for Ukraine, where territorial disparities and significant economic inequalities remain among the key challenges.

Ukraine, unlike the EU, faces a significantly more complex situation in the field of regional development. Under wartime conditions, some regions suffer from active hostilities, while others experience the destruction of infrastructure and the loss of economic potential. A substantial share of financial resources that should be directed toward recovery is instead allocated to security needs and maintaining macroeconomic stability amid Russia's military aggression. Therefore, the issues of post-war reconstruction and adaptation to European standards become central to the economic development policy discussed in the first subsection of this chapter.

To address these challenges, Ukraine must introduce or continue comprehensive reforms, in particular:

- decentralization, which provides regions with greater autonomy in addressing economic issues;

- development of public–private partnerships to attract investment into the regions;
- green recovery reforms, which promote sustainable development, environmental protection, and economic stability after the war.

At present, Ukraine is shaping a new state regional policy under the conditions of martial law. This process is based on the application of modern resource mechanisms of public administration and their legislative support in the complex environment of Russian aggression, as well as the implementation of European norms (regulations) in this sphere of public relations. The goal of this policy formation is to create conditions for preserving or restoring the quality of life, ensuring environmental sustainability, and maintaining state-guaranteed social standards for every citizen, regardless of place of residence [6].

Despite severe challenges, Ukraine has substantial opportunities for development, particularly through:

- active use of European funds and programs for recovery;
- strengthening institutional capacity at the local level.

It is important to note that the very concept of balanced development occupies a central place in modern scientific and applied discussions concerning the transformation of socio-economic systems in a globalized world. Its origins go back to international initiatives of the late twentieth century, aimed at finding an optimal balance between economic growth and environmental protection. A landmark reference point was the report of the World commission on environment and development chaired by G. Brundtland, ‘Our common future’ (1987), in which the concept of sustainable development – understood as the integration of economic, social, and environmental dimensions – was formulated for the first time. A further step was the adoption of Agenda 21 at the UN Conference in Rio de Janeiro (1992), followed by the adoption of the UN Sustainable development goals (2015), which acquired a universal character.

For Ukraine, which designated integration with the European Union as a strategic course (EU – Ukraine association agreement, 2014), the task of ensuring balanced development has acquired dual significance: on the one hand, it is a prerequisite for approximation to European political and economic standards; on the other, it is an internal challenge connected with economic modernization, wartime reconstruction, and strengthening competitiveness.

The economic foundations of balanced development in Ukraine are closely linked to the transition from an extensive model to an innovation- and resource-efficient one. According to domestic scholars (V. Heyets, T. Vasylytsev and others), a key factor is the formation of an innovation-driven economy in which knowledge-intensive technologies, digitalization, and green energy serve as drivers of development. Investment policy plays an important role, focusing on long-term projects for the modernization of infrastructure and the energy sector. European experience confirms that strategic investments in renewable energy and environmentally clean technologies form new competitive advantages (European green deal, 2019).

An essential component of the economic foundations is the support of small and medium-sized enterprises, which, according to the European Commission, account for more than 50% of GDP and two-thirds of jobs in the EU. For Ukraine, SMEs represent a key resource for the socio-economic resilience of regions, diversification of production, and the mitigation of the monopolized structure of the economy. The European charter for small enterprises (2000) serves as a model of policy aimed at creating a favorable business environment, and this experience is directly relevant for Ukraine.

The managerial foundations of balanced development involve a comprehensive transformation of the public administration system. State policy must be based on the principles of good governance: transparency, accountability, efficiency, and inclusiveness (Council of Europe, 2008). Strategic planning plays a key role and must integrate economic, environmental, and social components.

Ukraine's European integration course necessitates the implementation of the *acquis Communautaire* in the fields of environmental policy, energy efficiency, competition law, and public procurement. Directive 2009/28/EC 'On renewable energy sources', Directive 2012/27/EC 'On energy efficiency', as well as Directive 2001/42/EC "On strategic environmental assessment" have become fundamental benchmarks for national reforms. Proper adaptation of these acts not only ensures Ukraine's compatibility with the EU but also provides long-term conditions for sustainability.

At the same time, as noted by Western scholars (J. Meadowcroft, A. Lenschow, K. Steurer), balanced development is impossible without integrated governance that overcomes the sectoral fragmentation of policies [7]. For Ukraine, this implies the need to combine economic reforms with ecological modernization and social policy. In particular, the support of innovative clusters must be aligned with energy-efficiency measures, while

employment programmed must correspond with human capital development and the education system.

The issue of balanced development becomes particularly relevant in wartime conditions. A significant portion of resources is directed to defense, limiting the possibilities for investment in civilian sectors. However, the large-scale reconstruction that will begin after the cessation of hostilities opens a unique window of opportunity. As stated in the ‘Ukraine Recovery Plan’ (2022), reconstruction must be based on the principles of green transformation, digitalization, and institutional strengthening. The use of modern standards in construction, transport, and energy can lay the foundations for a new model of economic development.

An important managerial precondition is strengthening the role of civil society. European practice demonstrates that sustainable development is impossible without broad public participation in policy planning, implementation, and monitoring. The Aarhus convention (1998) guarantees the right of access to environmental information, participation in decision-making, and access to justice in environmental matters. For Ukraine, the involvement of civil society organizations, scientific institutions, and business associations becomes an important condition for transparency and accountability.

Thus, the economic and managerial foundations for establishing balanced development in Ukraine in the context of European integration form a holistic model of state modernization. It is based on economic innovation, strategic management, integration into the EU *acquis*, and active participation of civil society. The synergy of these factors creates the basis for long-term resilience, social justice, and increased competitiveness of Ukraine as a modern European state.

Scientific analysis allows us to conclude that Ukraine’s further recovery requires abandoning the traditional management model oriented toward administrative control and shifting to adaptive, inclusive, and transformative governance based on European standards. This will ensure not only the restoration of destroyed facilities but also the formation of an institutional, economic, and social foundation for long-term balanced development and Ukraine’s integration into the European space.

The analysis of the economic and managerial foundations for establishing balanced development in Ukraine in the context of European integration processes allows us to state that the strategic recovery of the state

must be based on a comprehensive combination of economic, social, environmental, resource, and institutional mechanisms.

Thus, Ukraine's recovery in the context of European integration should become not only a process of reconstruction, but also a long-term project of modernizing public administration and the economy aimed at achieving balanced development. This is precisely where the strategic opportunity lies to turn the crisis into a chance and ensure a new quality of statehood and sustainable integration into the European political, economic, and social space.

14.3. Public governance mechanisms for state reserves of material assets: recovery and security

In the current conditions of Ukraine's gradual recovery after wartime destruction and large-scale socio-economic losses, the issue of state provision with resources and reserves acquires special significance. This issue goes far beyond the traditional understanding of reserves as material-technical or financial stockpiles for emergency situations. It refers to the formation of an integrated system of strategic reserves that includes economic, social, human, technological, and institutional components capable not only of ensuring societal survival in crisis circumstances but also of creating the foundation for sustainable development.

In the context of European integration processes and increased security challenges, the issue of reserve provision gains a new quality: it becomes an element of public governance that integrates state institutions, business structures, civil society, and international partners into a single system of resource interaction. It is precisely due to scientifically grounded methodological approaches and effective governance mechanisms that reserves can be transformed into a strategic asset of the state, performing the functions of a stabilization buffer, a catalyst for recovery, and a factor of long-term security.

An important task is the rethinking of the state's role in the process of forming and using reserves. The experience of crisis periods proves that without a strong, well-coordinated, and transparent system of public governance, accumulated resources may remain ineffective, inaccessible to societal needs, or even become a source of social tension. At the same time, a properly constructed state reserving policy and its integration with market and international mechanisms can ensure the stability of economic processes,

enhance the country's adaptability to global challenges, and strengthen recovery potential.

Thus, reserve provision appears not as a technical or financial issue but as a complex scientific-managerial task that determines the quality of public policy, the level of national security, and the prospects of Ukraine's integration into the European space.

Under wartime challenges and post-war recovery, Ukraine has found itself in a situation where the issue of resource and reserve provision has acquired strategic importance. Reserves are not only a material-technical or financial basis for eliminating the consequences of destruction but also a component of national security, determining the state's ability to guarantee societal resilience, the continuity of governance processes, and the functioning of the economy. In the current conditions of European integration aspirations and the formation of new public governance institutions, Ukraine is compelled to develop qualitatively new approaches to the creation and use of reserves that meet the standards of the European Union while at the same time addressing the specific needs of recovery.

From a scientific perspective, reserve provision can be viewed as a multi-level system that encompasses planning, formation, management, and the use of reserves in emergencies and in the process of long-term development. The theoretical basis includes concepts of state resilience, crisis management, as well as models of sustainable development that imply not only the effective use of available resources but also the creation of mechanisms for accumulation, preservation, and rapid mobilization in crisis periods. Balanced development in this context is impossible without a properly organized system of reserves that covers both material (energy, food, construction materials) and non-material (institutional, personnel, organizational) elements.

The role of the state in this sphere is decisive. Only central public governance bodies are capable of ensuring the systemic nature, scale, and fair distribution of reserves that have societal significance. In this sense, the functions of the newly updated State agency for reserves management (SARM) become critically important [8]. SARM acts not only as an administrator of state reserves but also as a key coordinator among governmental structures, regional administrations, private companies, and international partners. In the process of Ukraine's recovery, the agency can perform the function of the 'backbone' of the reserve system, ensuring the

integration of national interests and the requirements of international cooperation.

Overcoming these problems is possible only through deep systemic reforms. First and foremost, it is necessary to expand the powers and institutional capacity of the SARM, transforming it into a strategic center for planning and coordination of the entire reserve policy. SARM should evolve into a structure that defines long-term needs, develops scenarios for potential developments, and coordinates interagency interaction. This requires the introduction of modern digital reserve management systems integrated with national public administration information platforms. Digitalization will enable continuous accounting, prevent inefficient expenditures, and ensure transparency for society and international partners.

It should be noted that within SARM operates the Ukrainian State Research Institute 'Resurs' (the Institute), which provides scientific support to the activities of the central executive authority in the field of reserve management. The Institute is intended to ensure comprehensive scientific and methodological, expert-analytical, and technological support for state policy in the field of strategic stock management implemented by SARM in accordance with the legislation of Ukraine [9].

Under current conditions characterized by martial law, destructive economic consequences, and the need for large-scale post-war recovery, the role of the Institute becomes particularly critical. Its activities ensure:

- effective formation, accumulation, and management of state reserves;
- modernization and digitalization of public administration processes in the field of reserves;
- scientifically grounded support for defense capability and the resilience of critical infrastructure;
- integration of Ukrainian practices into the European and global space of strategic reserve management [10].

At present, the Institute is being formed as a new-generation scientific and analytical center that combines research, forecasting, technological development, and expert support for state policy in the field of strategic reserves. Its uniqueness lies in the integration of fundamental science, applied research, and practical implementation through digital, technological, and legal instruments.

From the perspective of public administration, reserve provision is not merely a technical tool but a component of state security and recovery policy.

The formation of reserves requires strategic vision, long-term forecasting of societal needs, and consideration of potential risks and crisis scenarios. For example, fuel reserves should be created with regard not only to the current needs of the armed forces or municipal transport, but also to the prospects of developing energy independence. Food reserves must take into account both domestic consumption and Ukraine's obligations as an exporter of agricultural products. Medical reserves should be built on the principles of the European civil protection system (RescEU), which provides for rapid access to vaccines, medicines, resuscitation equipment, and field hospitals.

The United States of America maintains a separate strategic petroleum reserve, established in the 1970s, which is capable of compensating for disruptions in energy supply. The existence of such a reserve plays a critical role in ensuring energy security, which is extremely instructive for Ukraine as a country traditionally dependent on fuel imports. Such practices demonstrate that effective reserve provision must be based on long-term forecasts and include scenarios for even global crises.

In the European context, Poland is particularly close to Ukraine, having developed its own system of strategic reserves after joining the EU, integrated into European mechanisms. The Polish government pays special attention to food and fuel stocks, as well as health-related reserves, which proved effective during the COVID-19 pandemic and in responding to migration challenges. The Polish experience demonstrates that reserves can become an important instrument of regional stability, opening prospects for Ukrainian-Polish cooperation in this field.

Theoretically, resource and reserve provision can be considered as a comprehensive system that includes planning, formation, management, and use of reserves under both crisis and normal conditions of state functioning. It encompasses both tangible and intangible resources, including financial, human, and institutional components, as well as information and analytical management tools. A key aspect is a synergistic approach that ensures the integration of all types of reserves into a unified system operating on the basis of forecasting, strategic planning, and public administration. Such an approach makes it possible to ensure not only the state's responsiveness to crisis events, but also long-term resilience, reducing the risks of losses and inefficient use of resources.

It should be noted that the scholarly literature identifies several main categories of reserves. Material reserves include energy resources (fuel, electricity, gas), food stocks, construction materials, and critically important

equipment. Financial reserves encompass stabilization funds, special recovery budgets, international loans, and insurance mechanisms. Human resource reserves are formed through the mobilization of civil servants, specialists in critical sectors, and retraining and reskilling programs. Institutional reserves ensure the organizational and legal framework necessary for effective management, including specialized agencies and logistics systems. Information and digital reserves consist of data, forecasting systems, and analytical modules that enable operational and strategic decision-making based on up-to-date information. Comprehensive management of these reserves, their coordination, and integration into the public administration system form the basis for the long-term recovery of the state [11].

An analysis of the methodological foundations and the role of public administration in the field of resource and reserve provision for Ukraine's recovery provides grounds to assert that reserves are not only an instrument of financial and economic stability, but also an important factor in ensuring national security, societal resilience, and trust in the state under conditions of crisis challenges. It is through the system of public administration that legal frameworks, institutional mechanisms, and organizational models are formed, enabling an adequate level of accumulation, preservation, renewal, and effective use of strategic reserves. At the same time, the methodological approach to this issue requires consideration of the multidimensional nature of reserves – from financial and material to human, technological, and natural – which necessitates the integration of interdisciplinary knowledge and comprehensive cross-sectoral interaction.

The recovery of Ukraine after large-scale destruction and socio-economic losses is impossible without the formation of an integrated reserve management system that would combine state regulation with market mechanisms, international support, and civic initiative. In this context, public administration emerges not only as an administrative and legal instrument, but as a strategic coordinator of resource flows capable of harmonizing the interests of the state, business, and society. An important task is to ensure transparency, accountability, and openness in the formation and use of reserves, which is a necessary condition for preventing corruption risks, increasing the effectiveness of state policy, and strengthening public trust.

Scientific and methodological reflection on the role of the state in reserve management makes it possible to view reserves not as a passive stock of resources for emergency situations, but as an active element of

development and recovery strategy. Within this paradigm, reserves perform the function of a long-term investment and stabilization instrument that supports economic growth, guarantees security, and forms the potential for Ukraine's integration into the European space [12].

Thus, the role of public administration in the field of resource and reserve provision acquires decisive importance for the implementation of Ukraine's recovery strategies. It is intended not only to accumulate and preserve resources, but also to ensure their effective allocation in accordance with development priorities, societal needs, and international obligations. This constitutes the essence of the modern approach to reserve management: it should be regarded as a system-forming element of state recovery policy that combines economic rationality, social justice, and the security of vital activity and state-building.

References

1. Verkhovna Rada of Ukraine. Official web portal of the parliament of Ukraine. Available at: <https://zakon.rada.gov.ua/laws/main?find=2&user=a&org=1&typ=1%7C2&dat=20220224&datl=2>
2. Ivascu, L., Pislaru, M., Alexa, L., & Vorotin, V. (2024). The future of risk management. monograph. Intech open, 754 p. Available at: <https://www.intechopen.com/online-first/1176391>
3. Vorotin, V., & Prodanyk, V. (2024). Strategic vision of European state-building and the resource and environmental component of public administration cohesion in Ukraine. Public administration: concepts, paradigm, development, improvement, 6, 32–41. Pereiaslav.
4. Regulation (EU) 2021/1059 of the European Parliament and of the Council of 24 June 2021. Available at: <https://www.csi.org.ua/news/reglament-yevropejskogo-parlamentu-ta-rady-vid-24-cherhvnya-2021-roku-2021-1059/>
5. Vorotin, V. Ye. (2022). Organizational and legal mechanisms of public administration of resource support for economic development. In R. O. Stefanchuk (Ed.), Legislative support for the formation and implementation of state policy of Ukraine under martial law (vol. 2: economic security of the state, stimulation and support of the economy, pp. 68–83). Kyiv: Lyudmila publishing house.

6. Cabinet of Ministers of Ukraine. Resolution on approval of the state strategy for regional development for 2021–2027. Available at: <https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text>

7. Meadowcroft, J., & Steurer, R. (2013). Assessment practices in the policy and politics cycles: a contribution to reflexive governance for sustainable development? *Journal of Environmental Policy & Planning*, 20(6), 734–751. <https://doi.org/10.1080/1523908X.2013.829750>

8. Regulation on the state agency of Ukraine for reserves, approved by the resolution of the Cabinet of ministers of Ukraine of 15 April 2025. No. 435.

9. Charter of the Ukrainian state research institute “Resurs”, approved by the order of the state agency of Ukraine for reserves of 12 August 2025. No. 14.

10. Development program of the Ukrainian state research institute “Resurs” until 2027. Available at: <https://ndiresurs.gov.ua/news/03092025.html>

11. Vorotin, V. Ye., & Prodanyk, V. M. (2024). Resource and environmental component of regional governance under martial law in Ukraine: Strategy of European State-Building. *State Construction*, 2(36), 196–206. <https://doi.org/10.26565/1992-2337-2024-2-15>

12. Vorotina, N., Koval, O., Vorotin, V., Prodanyk, V., & Shynkarov, A. (2023). Legal foundations and features of public administration in the budgetary sphere in Ukraine and abroad. *Rivista di scienze giuridiche*, faculty of law, Catholic University of Milan, 2, 247–262. Available at: https://jus.vitaepensiero.it/download/dettaglio.php?id_download=494&ddoc=1

Chapter 15
***Europe's economic security in the era of artificial intelligence
and digital transformation***
(V. Zianko, T. Nechyporenko)

The rapid development of digital technologies and the implementation of artificial intelligence are radically changing the structure of economic processes, management models, and security systems at both the national and international levels. The European continent is at a crossroads of new opportunities and challenges: on the one hand, artificial intelligence tools stimulate productivity, and on the other, they create risks that potentially threaten economic security. In these conditions, traditional approaches to security, formed in the industrial or early digital era, are proving insufficient to effectively counter new threats, particularly in the areas of cybersecurity, digital sovereignty, and algorithmic governance. Given the above, the purpose of this chapter is to systematically examine the key challenges and opportunities associated with the transformation of economic security in the era of digital technologies and artificial intelligence.

**15.1. Economic security in the context of digital transformation:
theoretical and methodological discourse**

The concept of economic security has undergone significant changes in its development, adapting to transformations in the geopolitical, economic, and social environment. Its initial formation is closely linked to ideas of national security, in particular the socio-economic policy of US President Franklin Roosevelt, known as the ‘New Deal’, which emphasized the role of the state in ensuring the welfare of citizens during the Great Depression. Further international recognition of this concept was enshrined in 1985 in the resolution ‘International Economic Security’ at the 40th session of the UN General Assembly [6], which recognized the stability of socio-economic development as one of the key factors of global security. In contemporary

scientific discourse, the economic security of a state is interpreted in a multifaceted way, taking into account not only the protective function of the state, but also the need to ensure internal stability, development, and adaptation to global challenges. Thus, O. Pravdyvets [14] defines economic security as the highest function of the state, which consists in creating the preconditions for the sustainable development of the national economy, social welfare, and effective protection of citizens' interests. O. Dyachkov [10] proposes a systemic-structural approach, according to which economic security encompasses a set of elements and processes capable of ensuring the viability of the economy in conditions of instability. The military aspect is particularly relevant: in the works of O. Sokolov [17] and analytical reports of the NISD [13], economic security is considered as an indicator of resilience to military, financial, and social threats. According to this approach, economic security is the basis for long-term national survival in conditions of hybrid warfare, sanctions, and destruction of critical infrastructure. M. Samofalova and co-authors [15] propose a comprehensive vision of economic security as a category that combines economic independence, resilience to external and internal threats, the ability to self-develop, and the implementation of the state's strategic priorities. This approach integrates both classic security functions and requirements for economic adaptability and innovation. In turn, O. Fedoruk [20] emphasizes that in an open economy, economic security takes on a polysystemic character, formed on the basis of a combination of national priorities and the requirements of the international economic environment.

Based on the analysis of the scientific views presented, it can be concluded that in modern scientific thought there is a gradual shift in emphasis in the interpretation of economic security: from the traditional defense-oriented approach to a strategically oriented one, in which economic security is viewed as a multifunctional tool for ensuring the stability, adaptability, and economic self-sufficiency of the state in the face of global challenges.

The interpretation of the category of economic security in constantly changing conditions is characterized by the presence of inherent features that reflect its multifaceted and dynamic nature. Key attributes include balance, systemic stability, resistance to destabilizing factors, and the ability to effectively counter threats, which is synchronized with ensuring sustainable development and meeting the needs of key economic actors. The evolution of this category from a purely defensive, state-centric paradigm to a

proactive, multi-level, and development-oriented model indicates a fundamental transformation of its content. The modern paradigm emphasizes the efficient use of resources, economic freedom, and harmonious development.

Economic security is now positioned not only as a mechanism for preventing destructive influences, but also as a strategic tool for ensuring sustainable development, resilience, and adaptability to dynamic changes in the external and internal environment. In a multi-level system of its implementation – from individual and corporate to regional and national levels – a violation at one level (for example, a cyberattack on an enterprise) can cause cascading negative consequences at the macroeconomic level. This manifests itself in disrupted supply chains, declining employment, falling GDP, and deepening social instability. The high degree of interdependence between the components of the economic system makes it imperative to develop and implement integrated economic security strategies that reflect the dynamics and synergistic interaction of all levels of the economic system. In addition to basic definitions, modern conceptual approaches to economic security cover a variety of aspects.

As we can see, the approaches to economic security presented in Fig. 15.1 complement each other, forming a comprehensive understanding of this category as a multidimensional phenomenon that requires simultaneous attention to four key aspects: institutional strength (effective legislation and policy); structural stability (healthy macroeconomics and diversification); functional adaptability (system flexibility and effective management); social welfare (employment and population protection). It follows that effective economic security can only be achieved through the simultaneous strengthening of institutions, improvement of the economic structure, enhancement of adaptability, and ensuring the well-being of citizens.

Digital transformation is fundamentally changing the understanding of economic security by integrating new dimensions. Categories such as cybersecurity, cyber resilience, information security, and digital sovereignty are becoming particularly relevant. The rapid spread of digital technologies, the transfer of business processes to virtual space, and the growing dependence on information and communication infrastructure are creating new risks and challenges. These threats include: the escalation in the frequency and complexity of cyberattacks, the risks of leakage or compromise of confidential data, the dysfunction of important digital systems, and threats associated with the use of artificial intelligence,

blockchain technologies, and autonomous algorithms for destructive purposes.

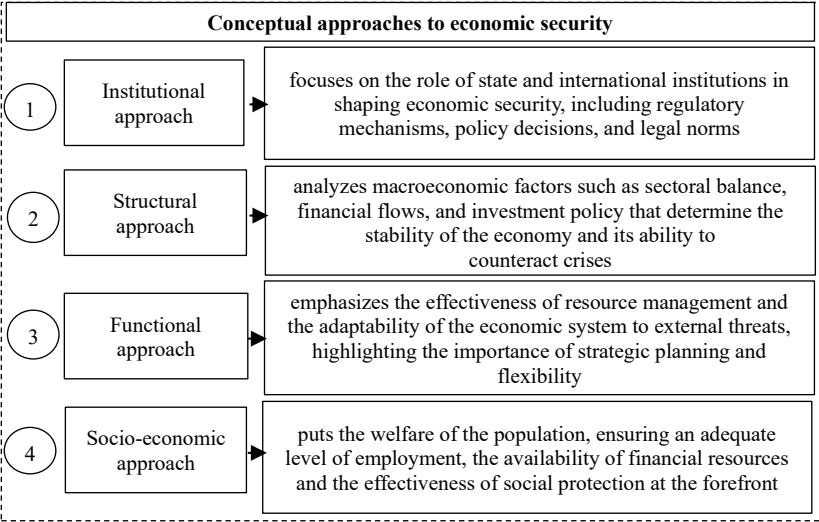


Fig. 15.1. Conceptual approaches to economic security

Developed by the authors

The modern paradigm of economic security requires the synthesis of traditional approaches with digital protection tools, the formation of an adaptive risk management system, and the development of proactive policies to respond to new types of threats caused by global digitalization. The diversity of scientific and methodological views on the essence and provision of economic security in the context of digital transformation is reflected in Table 15.1.

The approaches presented in Table 15.1 demonstrate that digital transformation is radically rethinking the concept of economic security.

It is no longer just protection against traditional threats, but encompasses the complex interaction of new challenges and opportunities, combining protection against digital threats, the development of innovative ecosystems, adaptation to technological changes, and the protection of national interests in the global digital space. This approach requires continuous monitoring of digital threats, active improvement of cyber hygiene, implementation of data protection systems, and ensuring business

continuity even in the event of cyber incidents.

Table 15.1

**Scientific and methodological approaches to defining economic security
in the context of digital transformation***

Author	Contents
Androshchuk G. [8]	The digital transformation of the European economy is changing traditional mechanisms for ensuring economic security, requiring new approaches to data regulation and protection.
Dluhopolskyi O., Simakhova A., Zatonatska T. [1]	The potential of the digital economy to ensure economic security in Europe lies in the creation of sustainable digital ecosystems and the integration of innovative solutions.
European Commission [2]	Digital transformation is a key factor in the EU's economic security, requiring policy harmonization, data protection, and the development of digital skills.
Grazevska N., Chygyrnskyi A. [9]	The digital transformation of the economy creates new risks and threats that require the development of mechanisms to protect national interests.
Kozlovsky S., Gorun S., Mamashvili L. [11]	Economic security of a state is the ability of the national economy to counter external and internal threats, ensure the stability of the financial system, and promote sustainable development through the introduction of innovative and digital technologies.
Kudrina O. [12]	The digital economy is changing traditional approaches to economic security, requiring new strategies for integrating digital technologies into public administration.
National Institute for Strategic Studies [13]	The digital transformation of Ukraine's economy promotes integration into the EU digital market, but at the same time requires mechanisms to protect national interests.
Silchenko V. [16]	Economic security in the context of digital transformation is determined by the state's ability to adapt to technological changes and ensure the stability of the economic system.
Storchak S. [18]	The impact of the development of the digital economy on the economic security of the state: strategic aspects and regulatory mechanisms.
Ukrainian Institute of the Future [19]	The digital economy is a key driver of global economic growth, affecting a country's economic security through market restructuring and technological challenges.

** Source: compiled by the authors*

The key principle is ‘resilience by design’, which involves integrating security mechanisms at all stages of the development and implementation of digital solutions. In addition to protection, these approaches promote the use

of digital technologies to strengthen economic security through innovative development and increased competitiveness.

15.2. Digital technologies and artificial intelligence: opportunities and threats to economic security

Economic security is the cornerstone of stability and prosperity for the European Union (EU) and its member states, providing protection against internal and external threats that could undermine national well-being and integration processes.

In the 21st century, under the influence of rapid digital transformation and the spread of artificial intelligence (AI), the architecture of European economic security is undergoing fundamental changes. Digital technologies and AI, while being powerful drivers of innovation, productivity, and competitiveness for Europe, also give rise to new and more complex challenges and threats. An analysis of the impact of these technologies for the period 2022–2024 shows their ambivalent role in shaping the economic security architecture of the union. Digitalization and AI open up unprecedented opportunities to strengthen the economic security of European countries by providing tools to improve the efficiency, transparency, and sustainability of their economic systems. They are key catalysts for innovation and productivity growth for the European economy. During 2022–2024, there will be a significant increase in the use of AI in European industry (particularly in Germany and France), finance (in centers such as London and Frankfurt), logistics, and other sectors. Automation of routine processes, optimization of production using robotics and advanced AI-based analytical systems enable European companies to significantly increase efficiency and reduce costs [2]. According to analysts, the introduction of generative AI, especially in recent years, is accelerating economic contribution in Europe by offering new opportunities for creating unique content, analyzing data, developing code, and interacting with voice interfaces [7]. This contributes to economic growth, increased GDP, and enhanced competitiveness.

The multifaceted and integrative role of artificial intelligence in strengthening the economic security of the European Union during 2022–2024 is clearly illustrated in Table 15.2, which demonstrates how its functionality covers various areas – from cybersecurity and finance to supply chain management and government regulation – providing systematic protection and increasing resilience. 15.2, demonstrating how its

functionality covers various areas – from cybersecurity and finance to supply chain management and government regulation – providing systemic protection and increasing resilience.

Table 15.2

Areas of application and functional impact of artificial intelligence on Europe's economic security (2022–2024)*

Scope of application in the EU	Example of AI functionality	Impact on Europe's economic security
Cybersecurity	Predicting and detecting cyberattacks (ransomware, phishing, DDoS) on European networks; automatic incident response; analyzing vulnerabilities in EU infrastructure.	Protecting critical European infrastructure (energy, telecoms, finance); preserving EU citizens' data; preventing financial losses from cybercrime in the region.
Financial sector	Fraud detection; credit risk analysis in European banks; monitoring transactions for money laundering in accordance with EU regulations; personalization of banking services.	Reduction in financial crime; increased stability of the EU banking system; trust in European financial institutions.
Supply chain management	Forecasting demand in European manufacturing companies; optimizing logistics within the EU and with partners; identifying vulnerabilities in European supply chains; monitoring geopolitical risks.	Strengthening the resilience of European supply chains to external shocks; ensuring the continuity of production and distribution of goods within the EU.
State management and regulation	Optimization of public services for EU citizens; big data analysis for EU policy-making; fight against corruption.	Improving the efficiency of the EU's administrative apparatus; reducing corruption risks, transparency in financial transactions.

* Source: compiled by the authors

Table 15.2 clearly demonstrates that AI is a powerful tool in the fight against cyber threats and financial crime, which is particularly important for the interconnected European financial system. AI-based systems are capable of analyzing vast amounts of data in real time, detecting anomalies and patterns that indicate potential attacks or fraud. Over the past three years, the EU has been intensively implementing AI solutions for [5]:

– proactive threat detection: AI algorithms predict new types of attacks by analyzing global trends and behavioral anomalies in European networks, which is critical for protecting the single digital market;

- combating financial fraud: the integration of AI analytics and behavioral biometrics has significantly improved the ability of European banks and financial institutions (e.g., in Luxembourg or Ireland) to counter fraud and money laundering, especially in line with strict EU regulatory requirements;

- automation of threat monitoring and analysis: this increases the effectiveness of protecting the economic interests of EU member states and European businesses.

In addition, digital transformation contributes to the creation of more flexible and resilient European organizations. The introduction of cloud solutions, remote workplaces, and AI systems for crisis management allows EU companies to better adapt to unpredictable circumstances, such as pandemics or geopolitical conflicts (e.g., the war in Ukraine, which has significantly affected Europe's energy security). This minimizes economic losses and ensures the stability of priority sectors of the European economy.

Along with opportunities, digital technologies and AI pose significant threats to the EU's economic security, requiring constant vigilance and the development of adequate countermeasures. Since 2022, Europe has seen a significant increase in the number and complexity of cyberattacks, including ransomware, phishing schemes, supply chain attacks, and data leaks. The increase in the number of vulnerabilities disclosed (according to the European Union Agency for Cybersecurity ENISA, their number has grown by 17% over the years analyzed [4]) reflects the constant growth of cyber risks in the region. Remote working and cloud technologies have expanded the attack surface, making end devices and data flows attractive targets for cybercriminals, often sponsored by aggressor states. The economic consequences of such attacks for the EU could be catastrophic, encompassing [7]:

- direct financial losses: ransom payments, system restoration costs, penalties for data breaches (high under the GDPR);

- indirect losses: loss of reputation, customer trust, business process downtime, impact on European stock markets;

- systemic risks: attacks on critical EU infrastructure (energy, transport, finance, healthcare), such as attempts to influence the energy systems of Germany or Poland, could cause widespread economic collapse (Table 15.3).

AI, being a powerful tool, poses new threats to European stability and security:

- AI-driven cyberattacks: attackers can use AI to automate attacks,

create more sophisticated viruses and phishing messages (in particular using deepfake technologies, which create risks of disinformation and manipulation of public opinion in the EU), and to identify vulnerabilities in security systems;

Table 15.3

Analysis of the destructive impact of digital technologies and artificial intelligence on Europe's economic security (2022–2024)*

Threat category	Description and impact on Europe	Example
Cyberattacks on the EU	The increasing number and complexity of attacks (ransomware, DDoS, phishing, APT) targeting European governments, companies, and critical infrastructure.	Attacks on European energy companies (e.g., in Finland or Romania); leaks of personal data of millions of EU citizens from government and commercial databases.
Vulnerability of European software and systems	Flaws in software and system configurations used in Europe that allow attacks and unauthorized access.	Identification of ‘zero’ vulnerabilities in European software products; increased risks for companies that have switched to remote working, particularly in the UK and Spain.
Using AI for attacks against the EU	Malicious use of AI to automate cyberattacks, create deepfakes for disinformation, and manipulate elections in Europe.	Phishing campaigns using AI for high levels of personalization; attempts to influence public opinion through deepfake videos during the European Parliament elections.
Ethical and social risks of AI in the EU	Algorithm bias, discrimination in social and economic processes, manipulation, job losses in key sectors of the European economy.	Controversy surrounding the use of AI in decision-making systems (e.g., credit scoring in France); discussions on the impact of automation on European labor markets, particularly in Scandinavian countries with high levels of automation.
Geopolitical risks and technological dependence	Competition for AI dominance among major players, risk of disruption to technology chains, cyber espionage against European institutions.	Pressure on EU countries regarding the choice of technology suppliers (e.g., disputes over 5G); concerns about dependence on non-European manufacturers of microchips and AI components, which is particularly relevant for the Netherlands (ASML) and Germany (investments in semiconductors).

** Source: compiled by the authors*

– ethical and social challenges: bias in AI algorithms can lead to discrimination in lending and employment in European companies, as well as manipulation of public opinion, undermining social and economic stability in the EU (it is worth noting that the European Union is a leader in the development of ethical standards and regulation of AI);

– unemployment risks and the transformation of the European labor market: automation and robotization, driven by AI, may lead to job losses in certain sectors of the European economy (e.g., manufacturing workers, data entry operators, drivers). This poses challenges for social stability and requires large-scale retraining and social protection programs;

– technological dependence and geopolitical risks: Europe's growing dependence on a limited number of leading AI technology developers (mainly the US and China) creates risks of geopolitical competition for digital dominance. This could lead to a 'split' in the global economy into technological blocs and affect European supply chains, access to critical technologies, and the EU's strategic autonomy.

Digital technologies and artificial intelligence play an ambivalent role in ensuring the EU's economic security. They open up unprecedented opportunities for innovation, productivity gains, and greater resilience for European economies. At the same time, their development creates new, complex threats that require constant adaptation, significant investment in cybersecurity, ethical and transparent regulation of AI, and intensified international cooperation. During the period under review, these trends have intensified, highlighting the EU's need for a comprehensive proactive approach to ensuring economic security. To function successfully in a dynamic environment, it is important for the EU not only to effectively counter threats, but also to optimally realize the potential of digital technologies and AI to strengthen resilience, stimulate innovation, and enhance global competitiveness.

15.3. Strategic approaches to ensuring economic security in the digital age

In response to the opportunities and growing threats associated with digital transformation and the development of artificial intelligence, the EU is actively developing and implementing comprehensive strategic approaches to ensure economic security. These approaches reflect the EU's desire to achieve digital sovereignty and strengthen strategic autonomy.

The EU is consistently strengthening cybersecurity, recognizing that cyber resilience is a prerequisite for economic stability. The emphasis is on multi-layered protection (perimeter, endpoints, networks, data), the implementation of Zero Trust principles, and enhanced threat information sharing between member states and European agencies. The NIS2 Directive plays a key role here, expanding the range of entities subject to cybersecurity requirements (covering, for example, food production, postal and courier services) and strengthening risk management requirements. The European Union Agency for Cybersecurity (ENISA) also provides important expert support and promotes cooperation. At the national level, countries such as Germany with its ‘Cybersecurity Strategy’ and France with the active development of national CERTs (Computer Emergency Response Teams) demonstrate a proactive approach to critical infrastructure protection [4].

The EU is a global leader in developing a comprehensive regulatory framework for AI – the AI Act, which was adopted in 2024 and will come into force in stages until 2026. This act sets a precedent in establishing global standards, classifying AI systems by risk level (from minimal to unacceptable), and setting strict requirements for transparency, ethics, safety, and oversight of ‘high-risk’ AI systems [3]. In particular, these include AI used in critical infrastructure, law enforcement, education, and employment. A key aspect is not only protecting citizens’ rights, but also ensuring trust in AI technologies, which is fundamental to their safe and sustainable economic use in the EU. In addition, clear regulation through the AI Act contributes to the creation of a predictable legal environment that stimulates investment in the development of safe and ethical AI solutions within the EU, preventing ‘regulatory arbitrage’ and supporting the competitiveness of European developers.

Recognizing the transformation of the European labor market under the influence of AI and automation, the EU and its member states are investing in retraining and training programs to prepare the workforce for the needs of the digital economy. In particular, this involves supporting STEM education, developing digital skills among the adult population, and creating ‘AI Academies’. For example, Spain and Italy are actively developing government programs to improve digital literacy, while the Netherlands is investing in specialized AI research centers [2]. The aim of these initiatives is to minimize the socio-economic risks associated with job displacement and to provide Europe with skilled workers for innovative development. It also contributes to increasing labor productivity and creating new, highly skilled

jobs in growing sectors, building a resilient and adaptable workforce that is fundamental to long-term economic security.

In addition to internal measures, Europe is actively cooperating with international partners (such as the US, Japan, and South Korea) to counter transnational cyber threats, exchange best practices, and develop common standards in the field of AI and cybersecurity. At the same time, the EU seeks to strengthen digital sovereignty by reducing its dependence on non-European technology giants. This is achieved through the development of its own digital ecosystems, including cloud computing (e.g., the Gaia-X initiative), semiconductor development (European Chips Act), and the development of its own AI solutions [2]. This strategy aims to ensure technological independence and protect Europe's economic interests in the face of growing geopolitical competition.

Conclusions. The economic security of European countries in the 21st century is taking on a new, multifaceted dimension, under the unprecedented influence of rapid digital transformation and the exponential development of artificial intelligence. This has fundamentally changed the paradigms of its conceptualization and provision. Traditional approaches are proving incapable of adequately responding to the dynamic spectrum of modern threats and fully utilizing innovative potential. This requires the formation of adaptive strategies and tools that take into account the digital reality.

Digital technologies and AI are catalysts for transformational change, bringing both enormous opportunities and significant threats to Europe's economic security.

On the one hand, they increase the competitiveness of European economies by stimulating innovative development, optimizing production processes, and enhancing efficiency in key sectors such as industry, finance, and logistics. In particular, in 2022–2024, the EU actively integrated AI solutions for cyber security, combating financial crime, and ensuring the continuity of critical business processes, which is fundamental to the stability of the single digital market.

On the other hand, digital transformation generates new, more complex and systemic threats. Analysis of the last three years shows a significant increase in the number and sophistication of cyberattacks that threaten critical infrastructure, government institutions, and the private sector. Direct and indirect financial losses from cyber incidents can be catastrophic for companies and national budgets. In addition, AI creates risks through its ability to automate and amplify cyberattacks (including disinformation

through deepfake technologies), and raises ethical and social challenges related to algorithmic bias, labor market transformation, and Europe's potential technological dependence on non-European technology leaders.

In response to these challenges and opportunities, the EU is taking a proactive and strategic approach to ensuring economic security in the digital age, which includes:

- comprehensive cybersecurity strategies: strengthening collective resilience by expanding coverage and cybersecurity requirements for critical sectors (in particular, Directive NIS2);

- EU Artificial Intelligence Act (AI Act): establishes the European Union's position as a global leader in shaping an ethical and safe framework for the development and implementation of AI, minimizing the risks associated with algorithmic bias, lack of transparency, and insufficient reliability of AI systems, while ensuring the protection of citizens' rights and economic interests;

- significant investment in digital skills and education: key to adapting the labor market and overcoming the risks of unemployment caused by automation;

- strengthening international cooperation and striving for digital sovereignty: reducing dependence on external technology giants and developing Europe's own digital ecosystems, particularly in the areas of cloud computing and semiconductors.

Thus, Europe's economic security in the era of artificial intelligence and digital transformation is a complex but manageable process. Its success depends on the EU's ability not only to effectively counter existing and new threats, but also to maximize the innovative potential of digital technologies and AI to strengthen resilience, innovative development, and global competitiveness. This requires constant adaptation of regulatory and strategic approaches, flexibility in responding to rapid technological change, and systemic investment in security and innovation.

Digital transformation and the development of artificial intelligence have fundamentally redefined the concept of economic security in the European Union, turning it into a multifaceted phenomenon. AI is both a powerful driver of economic growth and innovation, strengthening the EU's competitiveness and resilience, and a source of new, complex threats such as cyberattacks, systemic vulnerabilities, ethical dilemmas, and geopolitical dependence. Effective economic security for the EU in the digital age requires a proactive and integrated approach that combines institutional strengthening,

structural resilience, system adaptability, and citizen well-being with ongoing investment in cybersecurity, clear regulation of AI, and deeper international cooperation to ensure a stable and prosperous future.

References

1. Dluhopolskyi, O., Simakhova, A., Zatonatska, T. (2021). Potential of Digital Economy for Economic Security in Europe. *Advanced Computer Information Technologies*, No. 11, pp. 360–363.
2. European Commission. (2024). Report on the state of the Digital Decade 2024. Brussels: European Commission. Available at: <https://digital-strategy.ec.europa.eu/en/library/report-state-digital-decade-2024>
3. European Parliament and the Council. (2024). Regulation (EU) 2024/1689 on a common regulatory framework for artificial intelligence (AI Act). *Official Journal of the European Union*, L/2024/1689.
4. European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape, 2024. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
5. PwC. (2024). Global Digital Trust Insights Survey, 2024. Available at: <https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html>
6. United Nations. (1985). International economic security: resolution adopted by the General Assembly. A/RES/40/173. Available at: <https://digitallibrary.un.org/record/122626>
7. World Economic Forum. (2024). The Global Risks Report 2024. Geneva: World Economic Forum. Available at: <https://www.weforum.org/publications/global-risks-report-2024/>
8. Андрощук, Г. (2023). Цифрова трансформація європейської економіки: стан та місце України. *Інформація і право*, No. 4, С. 112–126. Available at: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0e6422b1-1215-421b-b171-05befac562b6/content>
9. Гражевська, Н., Чигиринський, А. (2021). Цифрова трансформація економіки в умовах посилення глобальних ризиків і загроз. *Економіка та держава*. <https://doi.org/10.32702/2306-6806.2021.8.53>
10. Дячков, О. (2022). Економічна безпека національної економіки: сутність, особливості, структура. *Економічні горизонти*, No. 1(19). С. 82–94. [https://doi.org/10.31499/2616-5236.1\(19\).2022.267022](https://doi.org/10.31499/2616-5236.1(19).2022.267022)
11. Козловський, С., Горун, С., Мамашвілі, Л. (2024). Підвищення

економічної безпеки держави на основі інноваційних та цифрових трансформацій. Економіка та суспільство, No. 59. <https://doi.org/10.32782/2524-0072/2024-59-34>

12. Кудріна, О. (2023). Цифрова економіка та економічна безпека. Digital Economy and Economic Security, No. 8, С. 183–187. <https://doi.org/10.32782/dees.8-31>

13. Національний інститут стратегічних досліджень. Базилюк, Я. Б. та ін. (2024). Економічна безпека України в умовах довготривалої війни: анал. доповідь. Київ: НІСД. <https://doi.org/10.53679/NISS-analytrep.2024.08>

14. Правдивець, О. (2022). Економічна безпека як найвища функція держави. Вчені записки Університету "КРОК", No. 2(66), С. 40–43. <https://doi.org/10.31732/2663-2209-2022-66-40-43>

15. Самофалова, М., Іванюта, Т., Сартаков, Д., Благодатний, А., Єременок, В. (2024). Сутність категорії "економічна безпека": структура та особливості формування. Київський економічний науковий журнал, No. 7. <https://doi.org/10.32782/2786-765X/2024-7-18>

16. Сільченко, В. (2024). Підходи до трактування дефініції "Цифрова трансформація". Економіка та суспільство, No. 66. <https://doi.org/10.32782/2524-0072/2024-66-132>

17. Соколов, О. (2024). Економічна безпека України в умовах воєнного стану. Науковий вісник Ужгород. нац. ун-ту. Серія: Право, Т. 1, No. 86, С. 41–55. <https://doi.org/10.24144/2307-3322.2024.86.1.41>

18. Сторчак, С. (2025). Вплив розвитку цифрової економіки на економічну безпеку держави. Економіка та суспільство, No. 71(1), С. 45–58. <https://doi.org/10.32782/2524-0072/2025-71-71>

19. Український інститут майбутнього. (2024). Країна з розвинутою цифровою економікою. Київ: UIF.

20. Федорук, О. (2023). Економічна безпека в умовах відкритої економіки: сучасні виклики та пріоритети державної політики. Економіка і держава, No. 5, С. 8–13.

Chapter 16

Intelligent systems for occupational safety supervision and management in European countries

(O. Krainiuk, Yu. Buts, M. Krainiuk)

The rapid advancement of digital technologies and the active integration of artificial intelligence (AI) present new opportunities for enhancing occupational safety standards, yet simultaneously give rise to a range of ethical, legal, and technical challenges. Traditional occupational safety methods are proving inadequate for effectively addressing the emerging risks within complex industrial and socio-technical systems. The core issue lies in the lack of holistic approaches to regulating, adapting, and implementing intelligent technologies within the domain of occupational safety. The objective of this paper is to analyse the key challenges and prospects of employing AI to develop a modern occupational safety model capable of ensuring proactive risk management and harmonisation with European standards.

16.1. The role of intelligent systems in the modern concept of occupational safety

In the 21st century, the issue of occupational safety has acquired a fundamentally new significance, as it is no longer confined to the boundaries of individual production processes or specific enterprises. The modern concept of occupational safety is integrated into the broader context of European security architecture, which encompasses a comprehensive system of protecting the individual from external and internal threats, as well as the formation of socio-economic conditions that guarantee stability, sustainable development, and a high quality of life. In this context, occupational safety is viewed as an integral component of the European civilisational model, at the centre of which stands the human being and their right to decent work in

conditions that do not threaten life and health. Modern concepts of occupational safety are integrated with the Sustainable Development Goals and are built upon multi-level strategies, where the human being is the central value. The ‘Occupational Safety and Health OSH 5.0’ model underscores the importance of the human factor amidst digitalisation and emerging risks [1].

Concurrently, the development of the modern economy is accompanied by dynamic changes that significantly influence the nature of the production environment. The deepening of specialisation, the increasing complexity of technological processes, the proliferation of automated and robotic systems, and the active implementation of digital platforms and ‘smart’ infrastructures create both new opportunities for increasing productivity and new risks for employees. The significance of information flows, the intensity of data processing, and the speed of managerial decision-making are increasing; precisely these factors determine the need for a transition from traditional approaches to systemic, flexible, and intellectually oriented safety management.

Classical methods for controlling and minimising occupational hazards, which rely primarily on regulatory compliance, periodic inspections, and statistical analysis, are increasingly revealing their limitations in contexts involving high-tech manufacturing or complex socio-technical systems. They are not always capable of ensuring a timely response to threats emerging in real-time, nor do they account for the non-linear nature of many production processes. Under these conditions, innovative tools emerge, capable not only of recording events but also of predicting their development, formulating risk prevention scenarios, and supporting managerial decision-making.

A distinct place among such tools is occupied by intelligent systems based on AI algorithms. They combine the capability to process large datasets, identify latent patterns, adapt to the changing conditions of the production environment, and optimise the risk management process. Unlike traditional information systems that operate according to pre-defined rules, intelligent solutions can learn, accumulate experience, and propose new action models in situations where the human factor is constrained by a lack of time or information.

Thus, the application of AI in the sphere of occupational safety constitutes not merely a technical innovation, but a conceptual step towards redefining the very paradigm of occupational safety [2]. This entails a transition from a reactive model, grounded in addressing consequences, to a proactive model focused on preventing hazardous situations and creating a

safe production environment throughout its dynamic development. In this regard, intelligent systems are viewed as a pivotal element of the 21st-century European safety architecture, integrating high technologies, regulatory standards, and humanistic values into a single, cohesive system.

Intelligent systems in the domain of occupational safety should be regarded as multi-level complexes of algorithms and technologies capable not only of recording hazardous events but also of providing analytical interpretation and forecasting, taking into account the dynamics of production processes. Their essence lies in the utilisation of AI, which, through machine learning methods and big data analysis, can identify latent patterns, model potential risks, and propose solutions aimed at mitigating the likelihood of emergencies [3, 4]. A distinctive feature of such systems is their capacity for self-learning – that is, continuous improvement based on accumulated experience – rendering them more flexible and effective compared to traditional approaches.

1. *Machine learning.* The utilisation of machine learning algorithms facilitates the identification of patterns and anomalies, as well as risk forecasting based on historical and contextual data. This ensures a timely response to threats and enhances the flexibility of supply chains, financial systems, and production processes.

2. *Integrated software solutions.* A systemic approach employing specialised software for risk analysis enables the management of uncertainty and improves the quality of information for decision-making, even in the presence of incomplete data [5].

3. *Multi-Criteria decision-making methods (MCDM/MCDA).* These methods permit the consideration of diverse risk factors, priorities, and expert opinions to select optimal measures within complex situations [6].

4. *Big Data and analytics.* The integration of big data and analytical algorithms (e.g., decision trees, NLP) enables a deeper analysis of risks, consideration of interrelationships between factors, and the formulation of effective management strategies [7].

5. *Stakeholder collaboration and digital platforms.* Networked collaboration models enhance the efficacy of risk prevention within digital ecosystems [8].

One of the key directions in the application of intelligent systems is the monitoring of employee status. Modern sensor technologies, combined with computer vision algorithms and biometric methods, facilitate the timely detection of signs of fatigue, stress conditions, or behavioural deviations that

may precede accidents. This provides the opportunity not merely to record the existence of a threat, but also to intervene promptly in the production process, thereby mitigating risks to human life and health.

Forecasting emergencies constitutes another crucial component. Based on historical data regarding incidents at enterprises, as well as through the modelling of potential behavioural scenarios of employees and equipment, AI systems are capable of identifying probable risk points in advance. This facilitates a transition from a reactive model, wherein actions are directed towards eliminating consequences, to a proactive one, which envisages preventing danger at its earliest stage [9].

Technologies aimed at analysing the technical condition of equipment are of particular significance. Intelligent predictive diagnostic systems are capable of monitoring machine operating parameters, identifying deviations from the norm, and forecasting the probability of failure. This minimises the risks of accidents associated with technical malfunctions and contributes to enhancing the reliability of production processes.

Among contemporary innovations, the creation of so-called digital twins of production warrants particular attention. These are virtual models of enterprises that provide the opportunity to replicate real-world processes within a digital environment, test various event development scenarios, and assess their potential consequences without detriment to the actual system. Such an approach significantly expands the safety management toolkit, as it enables the pre-emptive determination of optimal action strategies.

The application of intelligent systems in the domain of personnel training and development warrants particular attention. Modern simulators utilising virtual and augmented reality technologies are capable of modelling hazardous situations with a high degree of fidelity to real-world conditions, thereby fostering robust safety behavioural skills among employees. The integration of such educational platforms with personalised approach algorithms allows for the consideration of the individual characteristics of each employee, enhancing the efficacy of knowledge acquisition.

Thus, intelligent systems in occupational safety serve not merely as a technical tool, but as a holistic mechanism combining monitoring, forecasting, diagnostics, and training. They become the foundation for shaping a new safety culture oriented toward preemptive responses and the systemic protection of individuals within the modern production environment.

The implementation of AI creates new risks necessitating legislative adaptation and the strengthening of the role of employers and supervisory bodies. Flexible and responsive regulatory mechanisms are necessary to safeguard the mental and physical well-being of employees.

In contemporary Europe, the issue of occupational safety is regarded as part of a broader strategy for ensuring social and economic stability. Within the framework of European Union policy, occupational safety is closely linked to the concept of "decent work" and is integrated into pan-European sustainable development programmes. This determines the necessity not only to adhere to minimum occupational safety standards but also to form innovative mechanisms capable of responding to the challenges of high-tech manufacturing, globalisation, and digitalisation. In this context, AI-based intelligent systems are viewed as a promising tool for enhancing the effectiveness of safety management systems.

One of the key strategic benchmarks of the European Union is the 'Vision Zero' concept, which aims to eliminate fatalities and serious injuries at work. It is grounded in the idea that all accidents can be prevented if a systemic approach to risk management is applied. It is precisely intelligent systems that ensure the practical realisation of this concept: they allow for the prediction of potential threats, the identification of latent patterns in production process data, and the formation of models that reduce the probability of hazardous situations arising.

A pivotal direction involves integrating AI technologies into occupational safety management standards. The European standard ISO 45001, which specifies requirements for an occupational health and safety management system, is increasingly perceived not merely as a regulatory instrument, but as a foundation for the digital transformation of the manufacturing environment. The employment of intelligent algorithms within the framework of this standard facilitates the automation of data collection and analysis processes, ensures a responsive approach to shifting working conditions, and enhances the efficacy of internal audits.

Particular attention is also devoted to integrating intelligent systems within the scope of the 'Industry 4.0' industrial policy. This strategy envisages the digitalisation of all facets of production, including occupational safety. Owing to the advancement of the Internet of Things (IoT), cyber-physical systems, and cloud technologies, prerequisites are being established for the construction of 'smart factories', wherein occupational safety becomes an integral component of the broader digital ecosystem. Under such

conditions, the employee is safeguarded not only by traditional personal protective equipment but also by intelligent monitoring systems capable of recording their physical state in real-time, detecting hazardous environmental fluctuations, and transmitting alarm signals to central management platforms [10].

Large-scale pilot projects demonstrating the efficacy of this approach are already being implemented in several European countries. For instance, in Germany, ‘smart PPE’ systems – intelligent personal protective equipment integrated with sensors and mobile applications – are being widely deployed to ensure comprehensive monitoring of employees’ conditions [10]. In Scandinavian countries, particular emphasis is placed on the utilisation of digital platforms for risk management, where analytical models enable the prediction of injury rates and the development of strategies for their mitigation. France and the Netherlands are actively applying the concept of digital twins to replicate production processes and test behavioural scenarios of safety systems.

Collectively, these practices demonstrate that, within the European context, intelligent systems are evolving beyond their role as a mere auxiliary tool, transforming into a pivotal systemic factor that defines the future of occupational safety. They establish a new level of integration between technological, organisational, and legal mechanisms, creating the foundation for the safe development of the modern production environment.

Innovative tools – such as machine learning, big data analytics, multi-criteria methods, and digital platforms – significantly enhance the efficacy of risk prevention and managerial decision support within complex industrial and socio-technical systems (Fig. 16.1). Their implementation facilitates a timely response to emerging challenges and ensures the resilience of modern organisations.

Notwithstanding the substantial potential, the implementation of AI within the sphere of occupational safety is accompanied by a range of challenges, amongst which are ethical concerns (relating to the collection and utilisation of personal data), legal issues (determining liability for algorithmic decisions), and technical hurdles (ensuring data quality and reliable infrastructure) [11]. At the same time, these challenges present opportunities for harmonising legislation, developing standards, and creating innovative solutions that can enhance industrial safety.

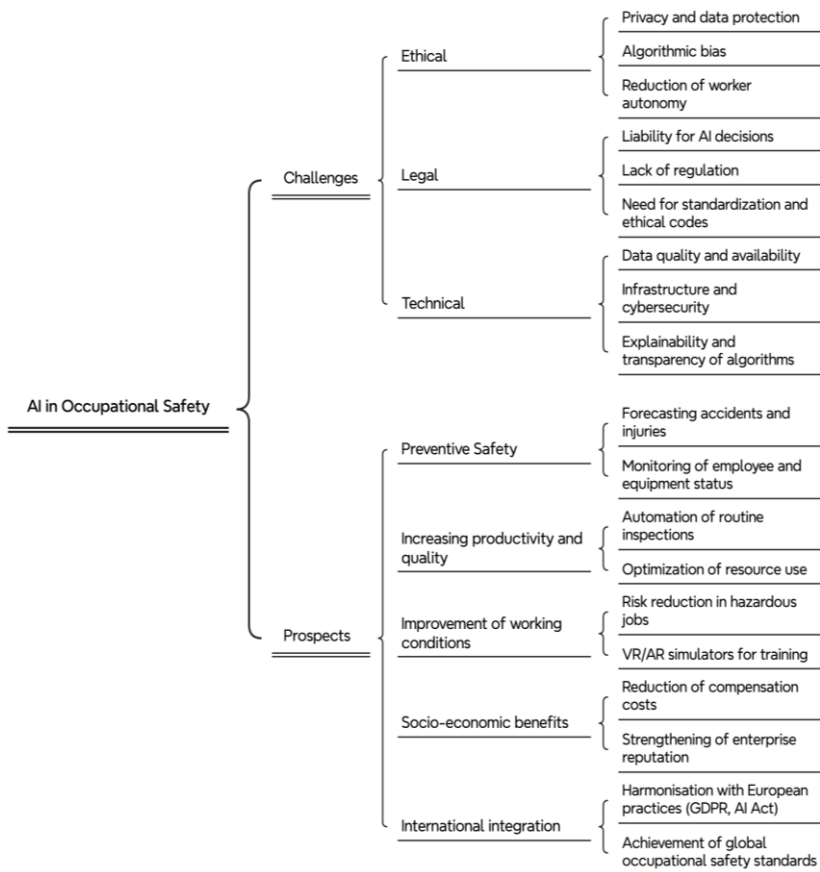


Fig. 16.1. Challenges and prospects for the implementation of artificial intelligence in the sphere of occupational safety

Compiled by the authors

In the 21st century, the concept of occupational safety is ceasing to be a localised sphere of managing individual risks. It is evolving into an integral component of the broader architecture of global and, specifically, European security. This process is driven by the integration of social, economic, and technological factors that dictate both the conditions of human existence in the world and the quality of professional activity. A safe production environment is viewed not merely through the prism of the physical

protection of the employee, but also in the context of the systemic resilience of enterprises, and the capacity of the economy to adapt to crisis challenges and respond to global threats, including those of a climatic, technological, and military nature.

The automation of production processes, the digitalisation of the economy, and the increasing technological complexity of industrial systems are shifting the emphasis within the traditional understanding of occupational safety. Whereas previously the key objective was the mitigation of injury probability through mechanical or organisational factors, the issue of managing complex risks currently assumes increasing prominence. This encompasses the monitoring of the technical condition of machinery and equipment, the analysis of the impact of working conditions on the physiological and psycho-emotional state of employees, the forecasting of emergencies, and the assurance of a prompt response to them. In this context, intelligent systems that combine artificial intelligence methods, sensor technologies, big data analytics, and cyber-physical solutions become not merely an auxiliary tool but a pivotal link in safety management.

The utilisation of such systems facilitates the formation of a new tier of preventive policy in occupational safety. Their efficacy stems from the capacity to integrate heterogeneous information flows – ranging from equipment performance indicators to biometric data regarding employee status – and transform them into actionable knowledge for operational management. This enables not merely a response to existing dangers, but the pre-emptive identification of potential threats, aligning with the contemporary paradigm of "anticipatory management". Through machine learning algorithms, such systems are capable of identifying latent patterns within the dynamics of production processes, modelling hazardous situation scenarios, and proposing optimal solutions for their prevention.

Concurrently, the role of intelligent systems is not confined solely to the technical and technological dimensions. They fundamentally alter the safety culture within enterprises, stimulating a transition from a reactive to a proactive model, wherein the responsibility for preserving the life and health of employees is shared among the individual, the collective, and automated systems. Such integration reinforces the interdependence between technical reliability, organisational resilience, and the human factor, shaping a multidimensional approach to occupational safety.

Thus, within the modern concept of occupational safety, intelligent systems act as a strategic resource combining technological capabilities with

humanistic objectives. They not only minimise occupational risks but also ensure the harmonious development of employees in interaction with the new industrial reality, where safety becomes an integral criterion for the sustainable development of society.

Development prospects lie in the creation of unified European standards for intelligent safety systems, as well as in the gradual integration of AI across all levels of risk management – from individual employee protection to the strategic safety programmes of states and corporations.

Intelligent systems are becoming a vital element of the contemporary architecture of European security, as they facilitate the combination of the technical capabilities of AI with the humanistic idea of protecting human life and health. The utilisation of AI in the sphere of occupational safety opens new horizons in the prevention of occupational risks, the formation of safe working environments, and the assurance of sustainable development in the 21st century.

16.2. European experience in implementing intelligent systems for occupational safety monitoring and management

European experience demonstrates a comprehensive strategy encompassing several key technological directions:

1. Predictive analytics systems. Instead of traditional post-factum analysis of accident causes, European companies employ machine learning algorithms to analyse big data sets. These data may encompass information regarding previous incidents, working conditions, climatic indicators, work schedules, equipment status, and even the physiological parameters of employees. AI models identify latent patterns and correlations, enabling the forecasting of risk probability under specific conditions. For instance, in the construction sector, such a system can determine an elevated risk of falling from heights at a particular site at a specific time of day, particularly under high humidity conditions.

2. Computer vision-based monitoring systems. The utilisation of cameras with embedded computer vision algorithms represents one of the most widespread solutions. These systems are capable of analysing visual data in real-time to detect violations of safety regulations. They can automatically identify whether employees are utilising personal protective equipment (PPE), such as helmets, goggles, or respirators [12]. Furthermore, they track deviations from safe movement trajectories, proximity to

hazardous zones, or the incorrect handling of industrial equipment. In the event of a violation being detected, the system automatically generates a notification, which can be sent to a supervisor or directly to the employee via a mobile application.

3. Internet of Things (IoT) and biometric technologies. The implementation of a network of sensors collecting data on the working environment and the physiological state of employees constitutes another pivotal component. Sensors integrated into workwear, wristbands, or equipment can monitor noise levels, vibration, temperature, and concentrations of harmful gases or dust. Biometric data, such as heart rate and stress levels, may indicate fatigue or a critical health condition [13]. All this data is transmitted in real-time to a centralised platform for subsequent analysis using AI.

Over the past 15 years, approaches to safety assurance in Europe have evolved from being predominantly regulatory to innovative, technologically driven methodologies. The experience of individual countries demonstrates that intelligent systems constitute not a unified solution, but rather one that adapts to the specificities of national economies and cultural idiosyncrasies.

In particular, Germany, with its robust industrial base and high culture of production, has concentrated on the integration of AI into engineering and manufacturing processes. Between 2019 and 2023, the proportion of German companies implementing AI rose from 6% to 13.3% [14]. Machine vision systems do not merely conduct monitoring but actively interact with robotics, facilitating ‘collaborative robotics’ (cobotics). For instance, on the assembly lines of automotive plants, AI-powered cameras track every movement of the worker. Should a person approach a hazardous zone or neglect to wear protective gloves, the system automatically reduces the robot’s speed or halts its movement, thereby preventing potential injury. This represents not passive surveillance, but a dynamic, interactive protection mechanism. Furthermore, predictive analytics has become an indispensable tool for maintenance. By analysing data from sensors embedded in machine tools (vibration, temperature, noise levels), AI algorithms are capable of predicting the probable failure time of key components with high precision. This allows for proactive maintenance rather than repair post-factum, significantly reducing the risk of accidents and production downtime.

The Scandinavian countries, particularly Finland and Sweden, where corporate social responsibility and employee well-being are prioritised, have placed emphasis on the psycho-emotional component of occupational safety

[15]. There is an understanding here that fatigue, stress, and professional burnout are among the primary causes of errors leading to accidents. Scandinavian companies are developing intelligent systems that analyse data regarding work schedules, holiday dynamics, as well as anonymised information on team interaction. These AI models seek patterns that may indicate early signs of stress, allowing management to intervene at an early stage – offering additional leave, psychological consultation, or redistributing the workload. This is a profoundly humanistic approach, demonstrating that care for the mental health of the employee is no less important than physical safety.

In France and other nations with advanced infrastructure, considerable interest has been generated regarding the application of intelligent systems for inspecting hazardous and inaccessible facilities. The French energy sector, in particular, actively employs drones equipped with thermal imaging cameras and computer vision algorithms for the monitoring of high-voltage power lines and substations. AI systems analyse imagery in real-time, detecting overheating, sparking, or insulation damage, which serve as precursors to potential accidents. Analogous technologies are applied within construction and bridge engineering, where autonomous robots fitted with sensors can examine load-bearing structures, identifying cracks or corrosion without necessitating human intervention at perilous heights or within confined spaces. This approach not only minimises risks but also significantly accelerates and enhances the precision of inspection operations. France stands as a leader in the deployment of intelligent systems for inspecting hazardous facilities, particularly in the realms of public safety and critical infrastructure [16]. The utilisation of AI, drones, and sensor technologies facilitates improvements in the efficiency, accuracy, and safety of inspections, whilst minimising human risk.

Practical experience demonstrates that the implementation of AI solutions within the sphere of occupational safety is not confined solely to major industrial powers. Thanks to technological innovations, even smaller European economies are discovering unique ways to enhance safety and efficiency.

In the United Kingdom, where the financial sector and office-based work constitute a significant proportion of the economy, the focus has shifted towards the intelligent monitoring of ergonomics and employee well-being. Systems utilising computer vision and sensors embedded within office furniture analyse the employee's posture, the duration of maintaining a single

position, and the frequency of breaks. Based on these data, the AI system can dispatch individualised recommendations regarding postural changes, the performance of warm-up exercises, or the necessity for rest [17]. This represents a proactive approach to preventing occupational diseases, such as carpal tunnel syndrome or back issues, which are prevalent among office staff. Such an approach significantly mitigates long-term health risks and, consequently, reduces corporate expenditure on treatment and compensation.

Spain and Italy, where agriculture and the construction industry constitute significant economic sectors, employ intelligent systems to enhance safety in open environments and under adverse climatic conditions. Here, AI helps monitor environmental risks. For instance, in agricultural operations in Spain, where the risk of heat stroke during summer is exceptionally high, intelligent systems analyse data from meteorological stations and GPS trackers installed on machinery [17]. AI is capable of forecasting hazardous conditions and automatically dispatching notifications to supervisors and employees, advising them to cease work and seek shade, thereby preventing overheating. In Italy, drones equipped with AI analytics regularly scan construction sites to detect violations, such as hazardously positioned materials or unstable structures, which can be of paramount importance in seismically active regions.

Finally, the Netherlands, renowned for its logistics and port infrastructure, is implementing intelligent systems for safety management within complex logistical chains [9, 16]. For example, at the Port of Rotterdam, AI algorithms analyse the movement of port cranes, lorries, and workers, preventing collisions and other incidents. The system can identify potentially dangerous manoeuvres and signal the crane operator or driver promptly, and in certain instances, even automatically adjust movement to avert an emergency. This constitutes not merely monitoring, but a system of dynamic risk management, wherein AI acts in the capacity of a ‘digital safety dispatcher’.

These examples demonstrate that intelligent safety systems in Europe are not solely a technological solution, but a flexible instrument that adapts to the unique requirements of each industry and country, confirming their pivotal role in shaping the future of occupational safety.

16.3. Integration of European approaches into the legal framework for occupational safety in Ukraine

The integration of intelligent systems for occupational safety monitoring and management necessitates a thorough study and adaptation of European legal experience by Ukraine. The regulatory foundation in the EU comprises the principles of prevention and data protection, enshrined, in particular, in the Framework Directive 89/391/EEC on measures to encourage improvements in the safety and health of workers at work and the General Data Protection Regulation (GDPR).

The Ukrainian regulatory framework is gradually aligning with European standards. The foundation is constituted by the Law "On Labour Protection" and the Law 'On Personal Data Protection'. These statutes stipulate general requirements for occupational safety and personal data processing; however, they lack explicit provisions regarding the utilisation of artificial intelligence or automated systems. In contrast to the GDPR, which strictly regulates the rules for data collection, storage, and anonymisation, Ukrainian legislation is limited to the requirement of consent for processing, without providing mechanisms capable of guaranteeing privacy protection. This creates legal uncertainty and additional risks for both employers and employees, particularly in instances involving the application of video analytics, facial recognition, or risk forecasting algorithms.

In the EU, the level of occupational safety requirements varies depending on the socio-economic specificities of the countries; however, a balance between safety and business expenditure is consistently maintained everywhere. For Ukraine, an additional challenge is the absence of explicit norms in the spheres of biometrics, video analytics, and risk forecasting algorithms: for instance, the application of facial recognition systems may precipitate conflicts with trade unions or incur sanctions from supervisory bodies.

Conversely, the EU is progressively establishing a detailed regulatory framework. The synthesis of directives and regulations establishes a sufficiently defined framework. The GDPR regulates the rules for personal data processing, Directive 89/391/EEC defines the preventive principles of occupational safety, while the AI Act classifies AI systems according to their risk level. In particular, technologies utilised for monitoring employee behaviour or for decision-making affecting their employment are categorised as high-risk and are subject to stringent requirements. In Ukraine, however,

general declarative formulations currently predominate, failing to provide sufficient legal guarantees for the implementation of innovations.

The development of intelligent systems in Ukraine is still in its nascent stage, whereas in EU countries, they have already become an integral component of production culture. Ukraine's potential lies in the high calibre of IT specialists, engagement in international research projects, and the activities of scientific schools capable of rapidly adapting modern digital solutions. This creates the prerequisites for the gradual implementation of cutting-edge technologies within industrial safety.

However, adaptation is hindered by a range of factors, including a lag in material and technical infrastructure, insufficient investment, and the tendency of many enterprises to focus solely on meeting minimum requirements. Conversely, in Europe, innovative systems are increasingly viewed as tools for enhancing productivity, mitigating risks, and strengthening business reputation. This distinction defines the fundamental disparity between the Ukrainian and European models of industrial safety development (Table 16.1).

As evidenced by comparative Table 16.1, a multi-level system of occupational health and safety regulation and data protection has already been established within the EU, explicitly accounting for digital technologies and AI (GDPR, AI Act). In Ukraine, however, the legal framework is primarily centred on general provisions without specific regulations regarding the utilisation of intelligent systems, thereby creating legislative gaps and legal uncertainty.

To integrate intelligent technologies into the sphere of occupational safety, Ukraine must simultaneously refine its legislative framework, taking into account European directives, and create economic conditions that incentivise the implementation of innovations. Only a combination of legal certainty and financial support will allow for the establishment of a modern occupational safety model capable of addressing the challenges of the digital era (Fig. 16.2).

The successful execution of these tasks will enable Ukraine to bridge the technological gap with the EU and utilise its own scientific and human potential to create a modern occupational safety model, wherein intelligent systems become a strategic safety instrument. In the event of inaction, the risks of lagging behind will only escalate, accompanied by an increase in occupational hazards and legal conflicts related to personal data.

Table 16.1.

Comparative table of EU and Ukrainian regulatory documents in the sphere of occupational safety and the use of AI

Area	EU	Ukraine
Occupational Safety	Framework Directive 89/391/EEC on measures to encourage improvements in the safety and health of workers at work (1989)	Law of Ukraine 'On Labour Protection' No. 2694-XII (1992)
Personal Data Protection	Regulation (EU) 2016/679 (GDPR)	Law of Ukraine 'On Personal Data Protection' No. 2297-VI (2010)
Artificial Intelligence	Artificial Intelligence Act (AI Act), Regulation (EU) 2024/1689 – classification and regulation of high-risk AI systems	National Strategy for the Development of Artificial Intelligence in Ukraine until 2030 (2020)
Privacy and Electronic Communications	Directive 2002/58/EC (ePrivacy Directive)	Law of Ukraine 'On the Basic Principles of Ensuring Cyber Security of Ukraine' (2017)
Occupational Safety Management System	ISO 45001:2018 (international standard, applied in EU countries)	Concept for Reforming the Occupational Safety and Health System in Ukraine (2019)

The analysis of the experience of European countries and the state of the legal framework in Ukraine demonstrates that intelligent systems are becoming not merely a technological tool, but a fundamental factor in redefining the very paradigm of occupational safety.

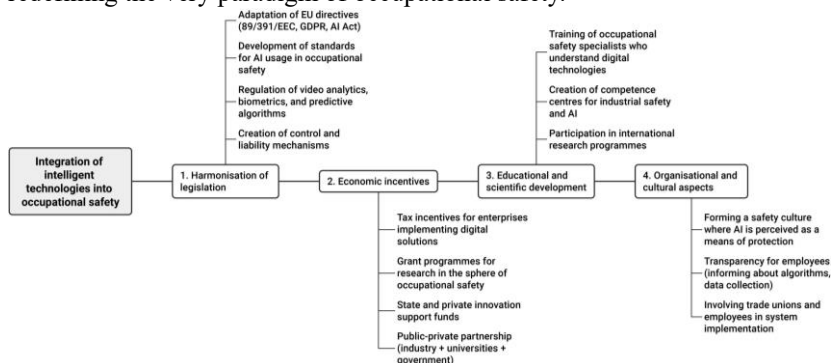


Fig. 16.2. Directions for the integration of intelligent technologies into the sphere of occupational safety in Ukraine

They are cultivating a new culture wherein the priority is not the remediation of consequences, but risk prevention and the integration of the technical capabilities of artificial intelligence with the humanistic values of protecting human life and health. Concurrently, the study has identified a critical challenge for Ukraine: the absence of a clear regulatory framework that would guarantee legal certainty and a balance between safety and personal data protection. This indicates that the future of occupational safety systems depends not so much on technical innovations as on the capacity of society and the state to integrate them into legal and organisational mechanisms, thereby ensuring synergy between technology, law, and social responsibility.

References

1. Крайнюк, О. В., Буц, Ю. В., Барбашин, В. В., Яцюк, М. В. (2023). Використання штучного інтелекту для управління безпекою праці. *Комунальне господарство міст. Науково-технічний збірник. Серія: Технічні науки та архітектура*. Т. 6, вип. 180. С. 207–214.
2. Крайнюк, О., Буц, Ю., Барбашин, В., Козодой, Д., Козодой, О. (2024) Інтелектуальні системи управління безпекою праці на основі штучного інтелекту: перспективи інтеграції в українське законодавство. *Комунальне господарство міст*. № 6 (187). С. 242–251. <https://doi.org/10.33042/2522-1809-2024-6-187-242-251>
3. Abdelaal, M. (2024). AI in Manufacturing: Market Analysis and Opportunities. *ArXiv*, abs/2407.05426. <https://doi.org/10.48550/arXiv.2407.05426>
4. Ávila-Gutiérrez, M., De Miranda, S., Aguayo-González, F. (2022). Occupational Safety and Health 5.0—A Model for Multilevel Strategic Deployment Aligned with the Sustainable Development Goals of Agenda 2030. *Sustainability*. Vol. 14, no. 11. P. 6741. <https://doi.org/10.3390/su14116741>
5. Buts, Y., Kagramanian, A., Kozodoi, D., Krainiuk, O., Hrytsenko, N. (2025). Ensuring the Safety of Enterprises Critical Transport Infrastructure Under Martial Law Conditions. In: *Intelligent Transport Systems: Ecology, Safety, Quality, Comfort. ITSESQC 2024*. Lecture Notes in Networks and Systems. Vol. 1336. Springer, Cham. P. 374–381. https://doi.org/10.1007/978-3-031-87379-9_34
6. El-Helaly, M. (2024). Artificial Intelligence and Occupational Health and Safety, Benefits and Drawbacks. *La Medicina del Lavoro*. Vol. 115, no. 2. <https://doi.org/10.23749/mdl.v115i2.15835>

7. Han, G., Pan, X., Zhang, X. (2024). Big data-driven risk decision-making and safety management in agricultural supply chains. *Quality Assurance and Safety of Crops & Foods*. Vol. 16, no. 1. P. 1445. <https://doi.org/10.15586/qas.v16i1.1445>
8. Huber, J., Anzengruber-Tanase, B., Schobesberger, M., Haslgrübler, M., Fischer-Schwarz, R., Ferscha, A. (2025). Evaluating User Safety Aspects of AI-Based Systems in Industrial Occupational Safety: A Critical Review of Research Literature. *International Journal of Environmental Research and Public Health*. Vol. 22, no. 5. P. 705. <https://doi.org/10.3390/ijerph22050705>
9. Ispășoiu, A., Miloșan, I., Gabor, C. (2024). Improving Workplace Safety and Health Through a Rapid Ergonomic Risk Assessment Methodology Enhanced by an Artificial Intelligence System. *Applied System Innovation*. Vol. 7, no. 6. P. 103. URL: <https://doi.org/10.3390/asi7060103>
10. Jarota, M. (2023). Artificial intelligence in the work process. A reflection on the proposed European Union regulations on artificial intelligence from an occupational health and safety perspective. *Comput. Law Secur. Rev.* Vol. 49. P. 105825. <https://doi.org/10.1016/j.clsr.2023.105825>
11. Komazec, N., Jankovic, K. (2023). A Systemic Approach to Risk Management: Utilizing Decision Support Software Solutions for Enhanced Decision-Making. *Acadlore Transactions on Applied Mathematics and Statistics*. <https://doi.org/10.56578/atams010202>
12. Krainiuk, O., Buts, Y., Kagramanian, A., Barbashyn, V., Yatsiuk, M. (2025). AI-Based Solutions for the Safe Transport of Dangerous Goods in the Context of Ukraine's European Integration. In: *Intelligent Transport Systems: Ecology, Safety, Quality, Comfort. ITSESQC 2024*. Lecture Notes in Networks and Systems. Vol. 1335. Springer, Cham. P. 236–247. https://doi.org/10.1007/978-3-031-87376-8_21
13. Li, Y., Wang, Y., Wang, L., Xie, J. (2022). Investigating the effects of stakeholder collaboration strategies on risk prevention performance in a digital innovation ecosystem. *Ind. Manag. Data Syst.* Vol. 122. P. 2045–2071. <https://doi.org/10.1108/imds-12-2021-0805>
14. Paman, H., Rogers, W., Behie, S. (2021). Selecting a method/tool for risk-based decision making in complex situations. *Journal of Loss Prevention in the Process Industries*. P. 104669. <https://doi.org/10.1016/j.jlp.2021.104669>
15. Rajkumar, S., Poddar, H., Harsha, S., Garg, Y., Shuraj, R., Vinodhini, M. (2024). Transforming Workplace Safety: The Intelligent Helmet Approach for Instantaneous Monitoring with Warning System. *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)*. P. 1–6. <https://doi.org/10.1109/AIIoT58432.2024.10574606>

16. Sánchez, S., Campero-Jurado, I., Herrera-Santos, J., Rodríguez, S., Corchado, J. (2021). Intelligent Platform Based on Smart PPE for Safety in Workplaces. *Sensors (Basel, Switzerland)*. Vol. 21, no. 14. P. 4652. <https://doi.org/10.3390/s21144652>

17. Trivedi, P., Alqahtani, F. (2024). The advancement of Artificial Intelligence (AI) in Occupational Health and Safety (OHS) across high-risk industries. *Journal of Infrastructure, Policy and Development*. Vol. 8, no. 10. <https://doi.org/10.24294/jipd.v8i10.6889>

Chapter 17

Corporate governance in the context of European security challenges

(G. Aleksin)

The European security environment after 2022 has fundamentally reshaped the framework of corporate governance. Security-related factors – ranging from energy supply disruptions and sanctions regimes to cyber threats and the growing requirements for non-financial data auditing – have become permanent input variables for supervisory boards and top management. This chapter examines how new regulatory regimes (NIS2, DORA, CER, CSRD/ESRS, CSDDD, CRMA, CBAM, the AI Act), the reconfiguration of the EU's energy supply, and the increasing “defense burden” across Europe are transforming decision-making structures, risk metrics, and the cost of capital for companies operating in finance, energy, industry, logistics, and digital infrastructure.

17.1. The European security context and corporate governance challenges

The contemporary European security environment is compelling corporate governance to move beyond traditional ESG-oriented frameworks and classical risk management. Since 2022, security considerations have become a structural element of business decision-making in Europe – ranging from energy pricing and supply-chain configuration to the protection of digital infrastructure, compliance with sanctions regimes, and the transparency of non-financial reporting. In 2024, NATO member states' defense expenditures reached historic levels: according to SIPRI [1], 18 of the Alliance's 32 members met or exceeded the 2% of GDP benchmark, while the average “defense burden” rose to 2.2% of GDP. Total NATO defense spending amounted to approximately USD 1.5 trillion, with European members accounting for around USD 454 billion. This trend signals a long-

term shift in the structure of public demand and investment priorities in dual-use industries, transport, logistics, cybersecurity, and materials science, indirectly affecting corporate strategies and the cost of financing.

The energy dimension of European security has undergone, over the past few years, the fastest transformation since the liberalization of the gas market. Eurostat data [2] indicate that the share of Russian sources in EU imports of natural gas via pipelines fell from 48% in Q1 2021 to 12% in Q2 2025, while the role of Norway and Algeria increased, helping to offset the reduction in supplies from the East. In the liquefied natural gas (LNG) market, the shift is even more pronounced: in Q2 2025, the United States accounted for 57.7% of EU LNG imports, whereas the share of Russian LNG declined to 12.9%. For corporate governance, this constitutes a tangible managerial challenge: companies must move away from inert, long-term contracting arrangements and operate with ‘live’ supply portfolios – managing terminal slots, freight markets, and a revised model of risk insurance – while considering sanctions constraints and heightened requirements for documenting the origin of raw materials. At the same time, in 2025 several EU countries, according to media estimates [3], continued to purchase Russian gas in substantial volumes, underscoring the complexity of fully unwinding historically established flows and reinforcing the need for compliance discipline and reputational oversight.

The EU sanctions regime is progressively shifting from static lists of prohibitions toward an engineering approach aimed at preventing the circumvention of imposed restrictions. In July 2025, the Council of the EU adopted the 18th sanctions package, which targeted Russian energy revenues, the banking sector, and the so-called shadow tanker fleet. Within this package alone, the number of sanctioned vessels associated with the shadow fleet was increased to 444, while the total number of individual listings exceeded 2,500; particular emphasis was placed on closing channels operating through third countries [4]. In autumn 2025, discussions focused on a 19th package intended to address remaining loopholes in liquefied petroleum gas (LPG) trade – specifically butane and isobutane – which had previously fallen outside the scope of certain sanctions measures.

From a corporate governance perspective, this shift has clear practical implications. Both financial institutions and non-financial companies are required to embed sanctions controls within a three-lines-of-defense framework. In this context, the European Banking Authority (EBA) issued unified guidelines in November 2024 on policies, procedures, and internal

controls for compliance with EU and national sanctions regimes [5]. As a result, sanctions compliance has effectively evolved into a formalized operational process with measurable performance indicators, rather than a purely declarative or “paper-based” component of internal policy.

The cyber domain has definitively moved from a purely technical sphere into the realm of governance. The NIS2 Directive [6] required Member States to transpose its provisions by October 2024, thereby activating a new regime that covers a broader set of ‘essential’ and ‘important’ entities and introduces personalized managerial accountability for risk management, incident response, and reporting. For the financial sector, the DORA Regulation [7] has applied since January 2025, embedding digital operational resilience into the business model of banks, insurers, investment firms, and critical ICT providers: supplier and contract registers, testing requirements, and incident investigation processes have become core agenda items for risk and audit committees within corporate governance structures. In addition, the Directive on the resilience of critical entities (CER) [8] extends the focus to physical resilience: EU countries must identify critical entities by mid-July 2026, while those entities must complete their own risk assessments and approve resilience-enhancement programs. In practical terms, this implies that security must be treated as an integrated system in which cyber and physical threats are assessed within a single, coherent risk matrix rather than managed as separate pillars.

The evolving profile of cyber threats is corroborated by empirical evidence. ENISA [9] reports that attacks – particularly distributed denial-of-service (DDoS) incidents – have become the most frequent threat vector, surpassing ransomware. In 2024, financial institutions experienced peak waves of DDoS attacks during specific periods, alongside a marked increase in chained attacks and social engineering. These trends significantly elevate the importance of time-based business continuity metrics – from recovery time objectives (RTO) and recovery point objectives (RPO) to the time required for detection and containment of incidents – as well as the discipline of resilience testing for service providers and the implementation of segmentation plans for critical services. From a corporate governance perspective, this translates into a question of the operational resilience of the business model itself, since in sectors with high digital intensity even brief service disruptions or performance degradation can have an immediate financial impact.

In parallel, at the level of values and enforcement, supply chain governance is undergoing a process of ‘mainstreaming’. The Corporate Sustainability Due Diligence Directive (CSDDD 2024/1760) [10], which entered into force in July 2024, establishes a phased application to large companies through 2029, shifting due diligence from a declarative exercise to enforceable responsibility for identifying, preventing, and remedying human rights violations and environmental harm within a company’s own operations and across its entire value chain [11]. Critical raw materials are addressed as a distinct policy pillar: the Critical Raw Materials Act (CRMA) [12] sets benchmarks for 2030 – at least 10% of extraction, 40% of processing, and 25% of recycling to take place within the EU – alongside a cap on dependency on any single third country of no more than 65% at any stage of the supply chain. The European Commission has already published lists of strategic projects, while heads of relevant agencies point to the need for at least EUR 10 billion in public funding for exploration and project development, with the potential to mobilize up to EUR 100 billion in private capital. Taken together, these developments are reshaping the business logic of industrial corporations: localization of processing, participation in recycling clusters, and long-term supply reliability agreements are increasingly becoming elements of board-level accountability, rather than merely matters of production technology.

The Carbon Border Adjustment Mechanism (CBAM) [13] will enter its full implementation phase in 2026 following the transitional period of 2023-2025. From the perspective of exporters to the EU, this entails not merely additional reporting requirements, but a genuine price signal linked to the carbon intensity of products; for European importers, it establishes mandatory procedures for the collection and verification of data on embedded emissions. In a context where carbon costs become an explicit component of the cost structure of imported materials, procurement, logistics, finance, and compliance functions must be integrated into a single governance framework. Failing to do so exposes companies to the risk of discrepancies between actual carbon footprints and the data subject to audited reporting.

The data and reporting agenda has become one of the strongest catalysts for changes in corporate governance practices. The first wave of companies is already reporting under the CSRD for FY2024, with publication in 2025; these are predominantly undertakings that were previously subject to the NFRD [14]. At the same time, the regulatory debate remains ongoing: the European Commission has proposed reducing the regulatory burden for

certain categories of companies and is reconsidering the phasing of application. Nevertheless, the broader trend toward assured and audited non-financial information continues to intensify – analytics platforms are already aggregating hundreds of first-wave reports across dozens of countries, while national authorities and audit firms are developing methodological approaches to test the coherence between non-financial and financial indicators [15]. From a corporate governance perspective, this means that ESG reporting is no longer an external, user-facing disclosure exercise; instead, it is becoming an internal data system that must be consistent with budgets, capital expenditure plans, and the firm’s risk appetite.

Another foundational governance pillar is artificial intelligence. The AI Act [16] entered into force in August 2024, with full applicability scheduled for August 2026. Certain obligations under the Regulation apply earlier: prohibitions on unacceptable practices and requirements related to AI literacy have been in effect since February 2025; obligations for general-purpose AI models apply from August 2025; and for high-risk AI systems embedded in regulated products, the transition period has been extended until August 2027. Despite market calls for a slower rollout, the European Commission confirmed in July 2025 that the implementation timetable would remain unchanged [17]. From a corporate governance perspective, this sends an unambiguous signal: companies must establish AI model registers, risk classification frameworks, data validation policies, and mechanisms for decision traceability in critical processes such as credit allocation, human resources, and compliance. Equally important is the alignment of contractual arrangements with AI model providers and cloud infrastructure suppliers with regulatory requirements, mirroring the approach already embedded under DORA in the financial sector.

The cost of capital in the Euro area declined somewhat in 2025, reflecting the pivot in the monetary policy cycle. In September 2025, the ECB [18] kept the deposit facility rate at 2.00%, marking a second consecutive pause following earlier rate cuts; markets largely interpreted this as confirmation of a controlled inflation trajectory. From a corporate finance perspective, this implies a lower discount factor in DCF-based valuation models, a more favorable window for refinancing, and renewed scope to restore investment portfolios focused on resilience and transformation. At the same time, regulatory and geopolitical risks continue to sustain elevated risk premia – particularly those associated with compliance, cyber resilience, and sanctions exposure – meaning that, in practice, ‘cheap’ financing for green or

transition projects is primarily accessible to firms able to demonstrate robust, evidence-based risk governance across energy systems, supply chains, and data management.

All the above is reshaping the day-to-day work of supervisory boards and top management. The first layer of change concerns the integration of cyber and physical resilience. Whereas IT risks were previously addressed largely at the technical level, under NIS2 [6], DORA [7], and CER [8] they are elevated to the remit of strategic and risk committees. This requires regular scenario-based resilience testing, clearly defined RACI matrices across business units, IT, security functions, and external providers, transparent metrics for detection and containment times, and recurring post-incident reviews with corresponding policy adjustments. ENISA data [9] indicate that even relatively ‘simple’ availability attacks can generate systemic effects when they coincide with peak demand periods or disruptions in third-party services. This, in turn, necessitates contractual obligations with providers covering incident reporting, recovery time commitments, and transparency regarding root causes. In the financial sector, DORA assigns particular importance to mapping IT dependencies and concentrations of risk with single providers. Already at the budget approval stage, boards are expected to review diversification plans, exit criteria, and service migration procedures that ensure continuity and regulatory compliance throughout the transition.

The second layer concerns supply chain governance as a legally binding obligation. The CSDDD [10] transforms traditional ‘supplier codes of conduct’ into enforceable due diligence requirements supported by evidence: registers of critical suppliers, mapping of human rights and environmental risks, and corrective action plans with defined timelines and accountable owners. From a corporate governance standpoint, this introduces traceability-based requirements: decisions to renew contracts with high-risk suppliers must be grounded in measurable progress in remediating identified violations, while payment structures increasingly depend on the successful completion of audits and assessments. The CRMA [19] adds an economic-geography dimension to this framework. Target benchmarks for extraction, processing, and recycling within the EU translate into a tangible matrix of investment projects in processing clusters, as well as a new logic for partnerships and M&A activity. Considering the strategic projects announced by the European Commission and the expected scale of public funding, companies are better served by entering consortia and establishing long

positions in critical raw material value chains, rather than attempting to ‘wait out’ volatility in spot markets.

The third layer concerns carbon costs as an operational KPI. CBAM, aligned with the gradual phase-out of ‘free’ allowances under the EU ETS, renders the ‘buy first, sort it out later’ approach prohibitively costly [20]. Companies importing steel, aluminum, cement, fertilizers, electricity, or hydrogen must therefore establish a coherent data architecture – from primary measurements at the production facility to consolidation within ERP systems and onward to report outputs subject to audited assurance. As a result, managerial decisions regarding suppliers cease to be purely “procurement-driven” and instead become inherently cross-functional: finance departments calculate the full cost base inclusive of CBAM-related charges, risk management functions assess sanctions and reputational exposures, and ESG teams ensure data validity and reporting compliance. This ‘triangle’ cannot function effectively without rigorous data discipline and verifiable, well-documented procedures.

The fourth layer is the institutionalisation of sanctions discipline. The EBA guidelines [5] have harmonized supervisory expectations regarding sanctions-related policies, procedures, and controls across all EU financial institutions, explicitly requiring sanctions screening to be embedded within the overall governance framework – from risk appetite setting to internal audit. For the real economy, the implications of the 18th sanctions package go beyond more complex payments or logistics: it introduces additional ‘red flags’ into due diligence processes, including exposure to the shadow fleet, high-risk ports, and transit jurisdictions [21]. Where contractual sanctions clauses may previously have been sufficient, current conditions increasingly require operational capabilities such as the rapid blocking of payments or shipments, decision logs, and time-based response metrics – reviewed by compliance functions and visible to supervisory boards.

At the sectoral level, the operating landscape is being reshaped almost across the board. In finance, DORA effectively provides a common language for the regulator, the bank, and the service provider: any incident affecting critical services must be addressed simultaneously at the technical and governance levels, and one without the other will not withstand scrutiny. Energy and heavy industry face stringent constraints from two directions – CBAM and the CRMA – and are therefore compelled to align decarbonization pathways with raw-material contracting strategies and processing capacity. For sectors such as telecommunications, transport, water

utilities, and healthcare, the combined implementation of CER and NIS2 means that video surveillance systems, industrial automation, and corporate IT can no longer be governed under separate protocols; they must be brought under a unified incident management and reporting architecture. All these processes carry an explicit cost dimension: in this context – alongside the ECB’s monetary cycle – the expected profitability of projects increasingly depends on the existence of an evidence-based risk governance framework [22].

The emerging trend is the convergence of compliance and operational execution. Without an agreed roadmap for sanctions and cyber controls across value chains, and without transparent ESG-CSR data, CFOs should not plan green investments; CROs cannot build a credible risk map in the absence of reliable data and auditable ESG-CSR procedures; CISOs cannot rely solely on “technical” policies without board-approved metrics and scenario testing; and procurement teams cannot run tenders without integrating CSDDD requirements. When these functions operate in a coordinated manner, a company’s cost of financing tends to decline – supported by a lower policy-rate environment, reduced regulatory risk, fewer incidents, and stronger confidence from creditors and investors.

Understanding this configuration makes it possible to frame competitive advantage as a deliberate operating-model choice rather than merely a matter of image. Companies that are first to ‘hardwire’ security into finance, operations, and data tend to capture market space more quickly in segments with regulatory-sensitive customers – from infrastructure operators and large retailers to firms in the pharmaceutical and aerospace industries. In the short term, this translates into stronger tender performance, lower insurance premia, faster bank approvals for financing limits, and higher readiness for independent assurance reviews. In the medium term, it supports more resilient cash flows by reducing the ‘risk tails’: fewer disruptions, a smaller share of losses from incidents and penalties, and less ‘idle’ capital tied up in single-provider or single-jurisdiction dependencies. In the long term, it creates the option to become a preferred partner in CRMA-related projects, secure priority access to processing capacity, and position the company as a ‘low-risk’ importer under the CBAM logic.

Beyond the continually evolving regulatory framework, corporate governance in Europe faces a cultural challenge: the need for a new discipline of evidence-based management. It begins with dependency mapping – identifying who provides critical services, which countries sit along key

flows, which nodes constitute ‘single points of failure’, and which AI models materially influence decisions on staffing, credit limits, or supplier selection. This discipline is then operationalized through board-level metrics reviewed on a quarterly basis: response times for incidents and the blocking of high-risk transactions; the share of contracts containing sanctions clauses; the proportion of critical materials with verified origin under the CRMA logic; the consistency of ESG data with budgets and management reporting; and the frequency and outcomes of resilience testing. It culminates in budgeting practices where ‘security’ is no longer treated as a discretionary cost line that can be cut without consequences, but as a structural component of the cost base that reduces the probability of major future losses. Publicly available sources – from ENISA and SIPRI reports to ECB communications and European Commission documents – provide sufficient evidence that this logic is not a passing trend, yet reflects a new economics of risk and accountability.

17.2. Implementation of a corporate governance architecture in response to security challenges in Europe

The implementation of European security rules must not devolve into a ‘paper compliance’ exercise; accordingly, top management and supervisory boards will need to change the very way decisions are formulated and evidenced. Today, NIS2, DORA, the AI Act, CSRD/ESRS, CSDDD (CS3D), the CRMA, and CBAM operate as an integrated framework: these legal and regulatory instruments define not only **what** must be done, but also **how** a company must demonstrate that risks are managed systematically – through artefacts, processes, data, and verifiable outcomes. The core governance shift is a move from fragmented policies to an integrated operating model in which the board’s oversight function, executive roles, data architecture, and suppliers’ contractual obligations are ‘stitched together’ into a single language of risk, resilience, and evidence. As a result, the company can engage regulators in the regulator’s own terms: deadlines, incident materiality criteria, testing plans, control matrices, and reporting outputs are mapped directly to EU acts and technical standards. This is precisely how compliance becomes a governance advantage rather than additional business friction. NIS2 elevates the accountability of the management body for cyber resilience and introduces new obligations for risk management and incident

reporting following transposition, which Member States were required to complete by October 2024 [23].

The first instrument that supervisory boards should introduce is a unified risk register. This should not be a back-office spreadsheet, but rather a central object of corporate governance, integrating cyber and ICT risks under NIS2/DORA, AI-related risks under the AI Act, environmental and social risks under CSRD/ESRS and CSDDD, as well as raw material and carbon risks under CRMA/CBAM. The register should be explicitly linked to business processes, assets, and suppliers; receive real-time inputs from incident management systems; and support formal escalation to the supervisory board based on triggers that mirror the ‘materiality’ criteria defined in the relevant EU acts. In the financial sector, this register must reflect the specific requirements of DORA: the management body bears ultimate responsibility for ICT risk management, business continuity, reporting, and testing. Accordingly, any material deviation – ranging from recovery times to the quality of incident logs – should enter board-level decision packs as a factual signal rather than an interpretative assessment. Since DORA has applied as an enforceable regime since January 2025, corporate governance bodies are well advised to formally reinforce their roles and RACI allocations in statutes, internal regulations, and policies at an early stage.

The second foundational solution is a unified incident intake infrastructure. This is not a contact center, but a single, standardized entry point for all events, automatically classifying incidents in line with NIS2 criteria and – where financial institutions are concerned – with DORA reporting formats, while generating notification templates for national competent authorities. In practice, this is implemented through an integrated ITSM/SecOps platform linked to the service and asset catalogue, with embedded definitions of ‘significant incidents’, internal notification SLAs, and controls over statutory external reporting deadlines. A pipeline configured in this way eliminates inter-functional disputes over whether an incident meets materiality thresholds and ensures that identical events follow identical escalation paths – from first-line response to executive management and the board. For financial institutions, this pipeline is further complemented by procedures for classifying major ICT-related incidents in accordance with DORA technical standards, so that reporting and external interactions do not depend on ad hoc or manual interpretation.

The third cornerstone is a threat-led resilience testing program governed at board level. The oversight function should not only see that security simulation exercises (e.g., Red Teaming) have been conducted, but also a remediation trajectory that is explicitly linked to the firm's risk appetite and funding decisions. Following the adoption of Commission Delegated Regulation (EU) 2025/1190 [24] – which specifies the criteria for selecting financial entities for TLPT, methodological requirements, the use of internal testers, and the modalities for mutual recognition – it is advisable for the board to approve an annual testing program with clearly defined control milestones: scope, scenarios, external providers, recovery time targets, and re-testing timelines. This approach helps avoid “one-off campaigns” and, crucially, converts TLPT findings into tangible investment priorities for resilience – priorities that the supervisory board can trace directly in the budget.

Artificial intelligence constitutes a distinct implementation stream. Following the entry into force of the AI Act in August 2024, the first prohibitions on ‘unacceptable’ practices began to apply in February 2025, while obligations for general-purpose AI models have applied since August 2025; subsequent phases for high-risk systems extend through 2026–2027. This implies that the management body should approve an AI governance policy that includes a model register, risk and impact assessment processes, data governance controls where required, and dedicated funding for a quality management system for high-risk uses. A practical implementation driver in this area is an AI management system (AIMS) aligned with ISO/IEC 42001 [25], covering scope definition, roles and responsibilities, access and data-source controls, maintenance of technical documentation, and a roadmap for conformity assessment. In parallel, the Commission is preparing a code of practice for GPAI as a soft-law reference point, which is particularly relevant for shaping internal standards before the full secondary framework is finalized. Given the timelines, supervisory boards should think in terms of a portfolio rather than isolated projects: models should pass through defined control ‘gates’ – from experimentation to production – only after completing risk and compliance assessments.

ESG and supply-chain governance are embedded into the same architecture through the CSRD and the CSDDD. The first ESRS reports (Commission Delegated Regulation 2023/2772 [26]) are being prepared under the double materiality approach, with the management body determining material topics, data-quality control standards, and the

boundaries of functional accountability. In practice, this is operationalised by building a ‘canonical’ sustainability data model: a mapped inventory of sources (internal systems, suppliers, auditors), validation rules, transformation logs, a role-based access model and change controls, and an explicit audit trail within internal audit processes. The CSDDD, which entered into force in July 2024, adds due diligence obligations related to human rights and environmental impacts across the chain of activities, requiring formal escalation and remediation mechanisms integrated into contracts and supplier portals. In this setting, due diligence is not a ‘supplier questionnaire’ but an end-to-end workflow: risk segmentation, evidence verification, corrective action packages with defined timelines, and enforceable remediation provisions – including, where justified, the right to unilateral termination.

CRMA and CBAM represent the geo-economic dimension of this governance architecture. Under Regulation (EU) 2024/1252 (CRMA) [19], the EU aims to reach, by 2030, internal benchmarks of at least 10% extraction, 40% processing, and 25% recycling of consumption within the Union, while limiting dependence on any single third country to no more than 65%. For the management body, this translates into a need for regular reviews of supply concentration risk maps, scenario modelling for ‘dual sourcing’, and the alignment of sourcing decisions with capital investment planning. CBAM, in turn, moves from the transitional reporting phase of 2023–2025 to the financial phase from January 2026: importers will be required to declare embedded emissions and purchase CBAM certificates. In 2025, the Commission proposed simplifications, including the possibility of postponing the purchase of certificates for 2026 to 2027 – an option that remains under discussion by the legislators [27]. From a corporate governance standpoint, the key is not to wait for the final wording of secondary legislation, but to secure budgets, calculation processes, and supplier contracts in advance so that carbon costs are incorporated into financial plans proactively.

To avoid the system becoming merely declarative, the board needs ‘live’ instruments that allow it to shape operations in practice. First, a board-level resilience and technology risk charter should be adopted, defining escalation thresholds, the right to obtain independent opinions, audit rights, and the mandatory cadence of quarterly sessions focused on the cyber environment, artificial intelligence, and supply chains. Second, the supervisory board should be equipped with an analytical dashboard built around a small set of

indicators that are difficult to ‘polish’: recovery times for critical services; the share of assets brought into compliance with baseline NIS2 controls; the on-time remediation rate of TLPT findings; the proportion of AI models that have completed conformity assessment – or, at minimum, an AIMS-aligned risk assessment; the share of ESRS data that has been verified; the budget allocation and status of CBAM certificates; and the trajectory of supply concentration risks measured against CRMA benchmarks. Third, governance should be reinforced through contractual ‘micro-circuits’: standardized annexes to contracts with ICT providers (audit rights, logging requirements, RTO/RPO, geo-diversification, and exit plans under DORA), with material suppliers (embedded-emissions data for CBAM, verification rights, and remediation/liability provisions under the CSDDD), and with AI developers (pre-deployment assessments, logging, transparency duties, and rights aligned with the AI Act). Viewed this way, oversight shifts from retrospective commentary to a proactive decision architecture structured as: ‘policy – process – data – contract – board dashboard metric’.

A distinct layer concerns the culture of assurance and learning. At board level, this requires a structured education program: concise briefings on regulatory developments; scenario-based ‘war room’ exercises addressing combined crises (cyber environment, physical infrastructure, information operations); and interactive tabletop simulations of crisis events incorporating incident-reporting mechanics aligned with NIS2/DORA. These activities are designed to refine coordination among the CISO, CRO, CIO, executives responsible for artificial intelligence and for CBAM/ESG, and business unit leaders. Public sources indicate that the European threat landscape is increasingly characterized by attacks on availability, ransomware, and the ‘camouflaging’ of malicious activity as legitimate services. Companies therefore need to model precisely these attack paths and test their capacity for rapid containment. Regular testing, standardized logs, and precise notification procedures are the only effective means of keeping pace with evolving threats.

Ultimately, implementing these requirements is a matter of process engineering. In concise terms, the board establishes an architecture in which NIS2 is translated into measurable controls and scenario-based testing; DORA into a live register of ICT providers and a budget-linked TLPT program; the AI Act into an AIMS framework and controlled gates for moving models into production; CSRD/ESRS into a canonical data model and internal audit; CSDDD into a due diligence pipeline with contractual

enforceability; CRMA into concentration risk maps and diversification plans; and CBAM into carbon cost calculations and a certificate calendar. When each of these building blocks is supported by clear artefacts, digital traces, and unambiguous roles, corporate governance moves beyond reactive compliance toward the active management of resilience and cost structures. This is the new norm of Europe's security era: board-level accountability for the genuine controllability of risks, evidenced through processes, data, and concrete actions on the calendar dates set by EU law.

References

1. SIPRI. Unprecedented rise in global military expenditure as European and Middle East spending surges. 2025. Available at: <https://www.sipri.org/media/press-release/2025/unprecedented-rise-global-military-expenditure-european-and-middle-east-spending-surges>
2. Eurostat. EU trade with Russia – latest developments. 2025. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=EU_trade_with_Russia_-_latest_developments
3. Reuters. EU sticks to planned Russian oil exit by 2028, energy chief says. 2025. Available at: <https://www.reuters.com/sustainability/climate-energy/eu-sticks-planned-russian-oil-exit-by-2028-energy-chief-says-2025-09-05>
4. European Commission. EU adopts 18th package of sanctions against Russia. 2025. Available at: https://finance.ec.europa.eu/news/eu-adopts-18th-package-sanctions-against-russia-2025-07-18_en
5. EBA. Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures. 2025. Available at: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/anti-money-laundering-and-counter-funding-terror-finance/guidelines-internal-policies-procedures-and-controls-ensure-implementation-union-and-national>
6. European Commission. NIS2 Directive: securing network and information systems. 2025. Available at: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
7. EIOPA. Digital Operational Resilience Act (DORA). 2025. Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
8. EUR-Lex. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and

repealing Council Directive 2008/114/EC. Available at: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng>

9. ENISA. ENISA Threat Landscape 2024. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>

10. EUR-Lex. Directive (EU) 2024/1760 of the European Parliament and of the Council of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859. 2024. Available at: <https://eur-lex.europa.eu/eli/dir/2024/1760/oj>

11. European Commission. Corporate sustainability due diligence. 2025. Available at: https://commission.europa.eu/business-economy-euro/doing-business-eu/sustainability-due-diligence-responsible-business/corporate-sustainability-due-diligence_en

12. European Commission. Critical Raw Materials Act. 2025. Available at: https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en

13. European Commission. Carbon Border Adjustment Mechanism. 2025. Available at: https://taxation-customs.ec.europa.eu/carbon-border-adjustment-mechanism_en

14. European Commission. Corporate Sustainability Reporting. 2025. Available at: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

15. European Commission. Proposal for a directive of the European Parliament and of the Council amending Directives (EU) 2022/2464 and (EU) 2024/1760 as regards the dates from which Member States are to apply certain corporate sustainability reporting and due diligence requirements. Available at: https://commission.europa.eu/document/download/0affa9a8-2ac5-46a9-98f8-19205bf61eb5_en?filename=COM_2025_80_EN.pdf

16. EUR-Lex. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

17. European Commission. European approach to artificial intelligence. 2025. Available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>

18. ECB. Monetary policy decisions – 11 September 2025. Available at: <https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.mp250911~6afb7a9490.en.html>

19. EUR-Lex. 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 and amending Regulations (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1724 and (EU) 2019/1020. Available at: <https://eur-lex.europa.eu/eli/reg/2024/1252/oj/eng>

20. Crowell. The EU CBAM Transitional Period Begins: A Practical Guide for EU Importers. 2023. Available at: <https://www.crowell.com/en/insights/client-alerts/the-eu-cbam-transitional-period-begins-a-practical-guide-for-eu-importers>

21. Fieldfisher. Key guidelines from the European Banking Authority on sanctions compliance. 2024. Available at: <https://www.fieldfisher.com/en/insights/key-guidelines-from-the-european-banking-authority-on-sanctions-compliance>

22. KPMG. Climate-related and environmental risks in loan pricing. 2023. Available at: <https://kpmg.com/xx/en/our-insights/ecb-office/climate-related-and-environmental-risks-in-loan-pricing.html>

23. European Commission. NIS2 Directive: securing network and information systems. Available at: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

24. EUR-Lex. Commission Delegated Regulation (EU) 2025/1190 of 13 February 2025 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the criteria used for identifying financial entities required to perform threat-led penetration testing, the requirements and standards governing the use of internal testers, the requirements in relation to the scope, testing methodology and approach for each phase of the testing, results, closure and remediation stages and the type of supervisory and other relevant cooperation needed for the implementation of TLPT and for the facilitation of mutual recognition. Available at: https://eur-lex.europa.eu/eli/reg_del/2025/1190/oj/eng

25. ISO/IEC 42001 – AI Management. 2023. Available at: <https://www.iso.org/ru/standard/42001>

26. EUR-Lex. Commission Delegated Regulation (EU) 2023/2772 of 31 July 2023 supplementing Directive 2013/34/EU of the European

Parliament and of the Council as regards sustainability reporting standards.
Available at: https://eur-lex.europa.eu/eli/reg_del/2023/2772/oj/eng

27. Normative. The EU's Carbon Border Adjustment Mechanism (CBAM), explained. 2025. Available at: <https://normative.io/insight/eu-cbam-explained>

Section 4

European Security and Ukraine

Chapter 18
***Ukraine as a key player in European security: geopolitical
and economic aspects***
(N. Lukianenko)

The twenty-first-century security architecture of Europe is undergoing a profound transformation, driven by interdependent challenges in energy resilience, digital governance, and infrastructural integration. Within this evolving landscape, Ukraine has transitioned from a peripheral geopolitical actor to a strategic contributor to the European Union's (EU) efforts to build a secure, autonomous, and interconnected regional order.

This chapter addresses the scientific problem of how Ukraine's functional integration into European energy, trade, and digital systems contributes to the EU's strategic resilience. While traditional analyses often frame Ukraine's role through the prism of geopolitical vulnerability, this study seeks to reframe the discourse by examining Ukraine's institutional convergence, infrastructural modernisation, and regulatory alignment with EU norms.

The research applies a mixed-methods approach, combining comparative policy analysis, statistical trend evaluation, and scenario-based modelling. Empirical data from EU institutions, Ukrainian government reports, and international think tanks are used to trace causal relationships between Ukraine's integration efforts and European security outcomes. For instance, the EU's Ukraine Investment Framework mobilised over €40 billion in public and private investments to support infrastructure and energy resilience across Ukraine's regions, directly contributing to European connectivity and stability [1, p. 3].

The chapter is structured into three analytical sections. The first explores Ukraine's geopolitical

positioning and its engagement in multilateral regional frameworks such as the Eastern Partnership and GUAM. The second assesses Ukraine's contributions to European energy security, trade networks, and transport infrastructure, drawing on recent data from the European Commission and the Vienna Institute for International Economic Studies. The third examines Ukraine's role in digital governance, cyber resilience, and critical infrastructure protection, including its participation in EU cybersecurity exercises and alignment with NIS2 and GDPR standards [2, p. 5; 3, p. 1].

By integrating statistical evidence and policy analysis, the chapter argues that Ukraine is not merely a beneficiary of European security systems but a co-architect of their strategic evolution. This perspective contributes to a more nuanced understanding of European security as a multidimensional and collaborative endeavour.

18.1. Geopolitical role and regional alignment

Strategic location and connectivity

Ukraine's geographic position at the crossroads of Central Europe, the Black Sea basin, and the South Caucasus has long defined its geopolitical relevance. Functioning as a bridge between the European Union (EU) and the Eastern Partnership region, Ukraine facilitates the movement of goods, energy, and information across key transit corridors such as TRACECA and the extended TEN-T network. This connectivity enhances not only regional trade but also the EU's strategic depth in its eastern neighbourhood [4, p. 42].

Recent infrastructure investments – particularly in rail, port, and road modernization – have reinforced Ukraine's role in pan-European logistics. Projects co-financed by the European Investment Bank and the Connecting Europe Facility have improved interoperability and reduced bottlenecks along the Baltic-Black-Adriatic axis. These developments contribute directly to the EU's objectives of open, secure, and sustainable connectivity [5, p. 3].

Multilateral engagement and regional cooperation

Ukraine's active participation in multilateral platforms such as the Eastern Partnership (EaP), GUAM, and the Black Sea Economic Cooperation

(BSEC) reflects its commitment to regional policy alignment. These frameworks enable coordinated action in transport, digital transformation, border management, and environmental security. Within the EaP, Ukraine has engaged in structured dialogues on justice, mobility, and infrastructure, fostering institutional compatibility with EU member states [6, p. 3].

Through GUAM, Ukraine promotes regional economic integration and digital governance, advancing shared goals of transparency and innovation. Trilateral and quadrilateral formats involving Poland, Lithuania, and Romania further enhance situational awareness and joint planning in border control and civil protection [7, p. 58].

Contributions to EU strategic autonomy and resilience

The EU's Strategic Compass and Global Strategy emphasise the need for strategic autonomy in the face of hybrid threats and infrastructural vulnerabilities. Ukraine's alignment with EU norms – through Association Agreement protocols and sectoral reforms – supports the Union's capacity to project stability and manage external risks. Functional integration in areas such as customs modernisation and border surveillance illustrates Ukraine's role in building interoperable governance structures [1, p. 19].

Ukraine's experience in energy diversification and cyber capacity development informs EU-level policy learning. Its contributions are not contingent on membership but on regulatory convergence and operational compatibility. This model of integration strengthens the EU's external resilience without over-reliance on third-country actors [8, p. 23].

Environmental and climate security cooperation

Security governance increasingly encompasses environmental risk management and climate resilience. Ukraine's cooperation with the EU in transboundary water governance, biodiversity monitoring, and pollution control adds a preventive layer to regional security. Participation in climate risk assessments and alignment with the European Green Deal reinforce the EU's sustainability objectives [9, p. 58].

Joint civil protection initiatives, including disaster risk reduction and early warning systems, improve preparedness for natural and technological hazards. These non-militarised forms of cooperation contribute to geopolitical stability across Europe's eastern frontier.

Institutional trust and normative convergence

Ukraine's integration into European security frameworks is underpinned by normative convergence in rule of law, democratic accountability, and transparency. Domestic reforms in judiciary

independence, anti-corruption, and public procurement build institutional trust with EU partners. As Dragneva notes, such alignment fosters informal security benefits, including regulatory interoperability and diplomatic engagement in sensitive policy areas [6, p. 7].

Importantly, Ukraine's trajectory is shaped by policy dialogue and technical cooperation rather than coercive alignment. This approach reflects the EU's preference for inclusive, rules-based regional orders and enhances the legitimacy of its external governance model.

18.2. Economic integration and security contribution

Energy infrastructure and regulatory alignment

Ukraine's energy infrastructure plays a pivotal role in European strategic resilience. Its geographic position at the intersection of the EU and the Caucasus–Caspian region enables it to function as a transit corridor for gas, electricity, and increasingly, hydrogen. The modernisation of Ukraine's pipeline and grid systems – guided by EU principles of unbundling, third-party access, and market liberalisation – has significantly improved interoperability with European energy markets [1, p. 2].

A landmark achievement was the full synchronisation of Ukraine's electricity grid with the Continental European Network in March 2022, completed in under three weeks despite wartime conditions. This integration, coordinated by ENTSO-E, enabled real-time balancing, frequency regulation, and emergency electricity exchanges with EU neighbours [2, p. 1]. By 2024, Ukraine had become a full member of ENTSO-E, marking its operational and regulatory compatibility with European standards [2, p. 3].

Ukraine's underground gas storage capacity - exceeding 30 billion cubic metres – offers seasonal flexibility and strategic buffering for EU states during supply disruptions. The European Commission's Ukraine Energy Support Fund has channelled over €2 billion into grid repairs and renewable capacity expansion, reinforcing both domestic and regional energy security [1, p. 4].

Ukraine's role in energy transition

Beyond hydrocarbons, Ukraine is aligning with the EU's Green Deal objectives through decarbonisation, renewable energy deployment, and smart grid integration. Pilot projects in hydrogen infrastructure, district heating reform, and solar electrification of public services (e.g. hospitals via the 'Ray

of Hope' initiative) illustrate Ukraine's dual contribution to sustainability and resilience [1, p. 5].

The EU–Ukraine roadmap for renewable gases, agreed in 2025, supports joint investment in biogas and hydrogen corridors, enhancing energy diversification and reducing carbon intensity across the region [1, p. 6]. These efforts position Ukraine as a partner in Europe's long-term energy transition, not merely a transit state.

Trade integration and value chain participation

Since the implementation of the Deep and Comprehensive Free Trade Area (DCFTA) in 2016, Ukraine has reoriented its trade flows toward the EU, with over 60% of exports now directed westward. This shift has been accompanied by diversification into high-value sectors such as agri-tech, mechanical engineering, and chemicals [3, p. 17].

Ukraine's integration into EU value chains enhances economic security by stabilising industrial output, facilitating technology transfer, and supporting strategic autonomy in manufacturing. For example, Ukrainian metal components and agri-food inputs are critical to EU construction and food systems [4, p. 68].

Statistical data from the Vienna Institute for International Economic Studies shows consistent growth in Ukraine's exports of machinery and transport equipment, rising from 14.2% in 2018 to 18.1% in 2023, despite wartime disruptions.

Transport infrastructure and regional connectivity

Ukraine's participation in the Trans-European Transport Network (TEN-T) and the Connecting Europe Facility (CEF) has catalysed multimodal infrastructure development. Projects include rail electrification, port upgrades (e.g. Chornomorsk), and intermodal hubs linking inland waterways with freight corridors [6, p. 2].

In 2024, the EU allocated €7 billion to 134 transport projects, several of which directly support Ukraine-EU Solidarity Lanes. These include capacity upgrades at border crossings, integration of Ukrainian rail systems with EU standards, and digitalisation of customs procedures [6, p. 3].

Such infrastructure investments serve strategic purposes:

- supply chain diversification: reducing dependency on single routes and chokepoints;
- economic cohesion: fostering balanced development in border regions;

– emergency mobility: enabling secure transport of essential goods during crises.

Financial and investment integration

Ukraine’s financial architecture is increasingly embedded in European mechanisms. Between 2021 and 2024, over €3 billion in EU development financing supported energy efficiency, SME competitiveness, and digital infrastructure [1, p. 7].

Institutional reforms in public procurement, anti-corruption, and investment protection have improved Ukraine’s regulatory credibility. These changes encourage private sector engagement and reinforce the legal foundations of economic security [4, p. 8].

Integration into EU regulatory and statistical frameworks

Ukraine is progressively adopting EU technical regulations, statistical formats, and industrial standards. Cooperation with Eurostat and participation in twinning projects enable harmonisation in sectors such as pharmaceuticals, food processing, and engineering [3, p. 44].

This regulatory convergence reduces technical barriers to trade and supports mutual recognition of standards. It also allows Ukraine to contribute to the shaping of regional norms, rather than passively adopting them.

18.3. Digital and infrastructure security

Alignment with EU digital governance frameworks

Ukraine’s digital transformation is increasingly aligned with the European Union’s regulatory frameworks, particularly in the domains of data protection, cybersecurity, and digital infrastructure. The gradual incorporation of the General Data Protection Regulation (GDPR) principles into Ukrainian legislation has enhanced interoperability with EU data flows and cross-border services. The recognition of Diia. Signature under the EU’s eIDAS Regulation marks a milestone in legal and technical convergence, making Ukraine the first non-EU country with a digitally recognised signature across the Union [6, p. 2].

In parallel, Ukraine has adopted national cybersecurity standards modelled on the EU’s Directive on Security of Network and Information Systems (NIS2). These include mandatory risk assessments, incident reporting protocols, and classification of essential digital service providers. This alignment enables Ukraine to participate in EU-wide threat monitoring

and early warning systems, strengthening shared situational awareness [4, p. 1].

Participation in joint cybersecurity and resilience mechanisms

Ukraine's cybersecurity governance has matured through structured cooperation with EU institutions. The country actively participates in the EU–Ukraine Cyber Dialogue, which facilitates joint planning, legislative alignment, and operational coordination. The third dialogue, held in Brussels in July 2024, focused on strengthening cyber diplomacy, critical infrastructure protection, and the use of the EU Cyber Diplomacy Toolbox [4, p. 1].

Ukraine also engages in joint cyber exercises with ENISA, CERT-EU, and the European External Action Service (EEAS), simulating real-time incident response and cross-border coordination. These exercises build institutional capacity and ensure compatibility with EU civil and military cybersecurity protocols [1, p. 1].

Flagship projects such as CyberEast and EU4DigitalUA have supported Ukraine's cyber resilience through training, technical assistance, and legislative harmonisation. These initiatives have helped Ukraine develop sector-specific cybersecurity policies in energy, finance, and transport [6, p. 3].

Modernisation of critical infrastructure

Digital integration is closely linked to the resilience of critical infrastructure systems. Ukraine's efforts to modernise its energy grid, telecommunications networks, and transport systems are coordinated with EU investment and regulatory instruments. Smart grid deployment, supported by ENTSO-E and the European Bank for Reconstruction and Development (EBRD), enables predictive maintenance and cyber-attack detection, reducing system fragility [2, p. 202].

In telecommunications, convergence with the EU's Electronic Communications Code has improved market transparency and enabled secure 5G deployment. Infrastructure sharing and spectrum allocation reforms have reduced vulnerabilities in mobile data services [6, p. 3].

Transport systems have been digitalised through the adoption of electronic customs declarations (e-CMR), real-time freight monitoring, and corridor mapping. These upgrades enhance logistics security and interoperability with the EU's Intelligent Transport Systems (ITS) directive [5, p. 44].

Strategic value of digital sovereignty and interdependence

Ukraine's strategic importance in Europe's digital ecosystem lies in its functional contributions to EU-wide resilience. With over 250,000 ICT professionals and a growing export base in software and cybersecurity, Ukraine strengthens Europe's digital autonomy. Its adherence to EU standards in data localisation, privacy, and service continuity fosters mutual trust in cross-border digital transactions [6, p. 4].

Rather than pursuing digital self-sufficiency, Ukraine has embraced digital interdependence grounded in open platforms and shared protocols. This approach aligns with the EU's vision of a collaborative digital single market and reinforces the credibility of Ukraine as a trusted partner.

Institutional partnerships and capacity building

Capacity development is central to Ukraine's digital security strategy. Twinning projects with EU member states, joint curricula with European universities, and public-private partnerships on secure cloud infrastructure have built domestic expertise and embedded Ukrainian professionals in Europe's digital community [6, p. 5].

Participation in programmes such as EU4Digital and DT4UA has supported broadband access, digital literacy, and open science platforms. These initiatives not only improve service delivery but also cultivate a generation of cyber-aware decision-makers capable of sustaining long-term resilience.

18.4. Strategic outlook and future scenarios

Ukraine's role in the future European security architecture

As the European Union (EU) redefines its strategic posture in response to evolving threats, Ukraine's integration trajectory is increasingly viewed through the lens of long-term security planning. The EU's Strategic Compass and the Joint Security Commitments signed in June 2024 articulate a vision of Ukraine as a contributor to European defence, resilience, and institutional coherence [1, p. 2].

Ukraine's participation in the Common Security and Defence Policy (CSDP) missions, its alignment with EU defence procurement standards, and its cooperation with NATO structures position it as a future anchor of regional stability. The EU-Ukraine Defence Industries Forum, held in Brussels in May 2024, marked a turning point in industrial cooperation, with over 400 stakeholders identifying joint ventures and flagship projects to

integrate Ukrainian defence capabilities into the European Defence Technological and Industrial Base (EDTIB) [2, p. 1].

The establishment of the EU Defence Innovation Office in Kyiv further institutionalises this partnership. Acting as a coordination hub, the Office supports joint research and development, identifies bottlenecks in defence innovation, and facilitates Ukraine’s participation in future EU defence programmes [3, p. 1].

Fig.18.1 presents a chronological overview of Ukraine’s integration into the European security architecture between 2020 and 2025. The timeline highlights key institutional and policy milestones, beginning with the implementation of the Association Agreement and culminating in the launch of the Investment Framework and Civil Protection Mechanism. Each stage reflects a deepening of strategic alignment, from cybersecurity cooperation and energy grid synchronisation to foresight-based planning and joint resilience initiatives. This progression illustrates Ukraine’s transition from a peripheral partner to an active contributor in shaping regional security norms, with implications for both EU policy coherence and Ukraine’s long-term strategic positioning.

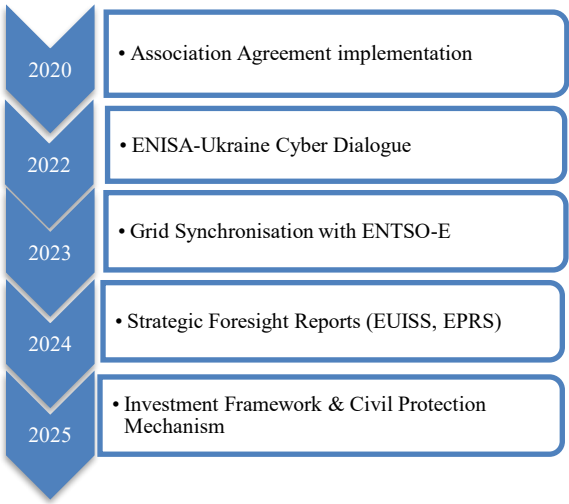


Fig. 18.1. Timeline of Ukraine’s Integration into EU Security Architecture

Compiled by the author based on [4, 7, 12]

This timeline reflects a cumulative deepening of strategic alignment, with each phase reinforcing Ukraine’s operational compatibility and normative convergence with EU frameworks.

Civil protection and disaster resilience cooperation

Ukraine’s accession to the EU Civil Protection Mechanism in April 2023 has expanded its role in European disaster preparedness and emergency response. As a full member, Ukraine now contributes to and benefits from coordinated deployments, shared expertise, and pooled resources across the EU and participating states [4, p. 1].

The Mechanism has enabled Ukraine to receive over 155,000 tonnes of emergency aid, including power generators, medical equipment, and water treatment systems. It has also facilitated the evacuation of over 4,000 patients to European hospitals via the EU Medevac Hub in Rzeszów [4, p. 2].

Table 4.2 outlines key milestones in EU–Ukraine cybersecurity cooperation from 2022 to 2025. These initiatives reflect a progressive deepening of institutional engagement, beginning with the ENISA–Ukraine Cyber Dialogue and culminating in the Strategic Cybersecurity Investment Plan led by the European Commission. The trajectory demonstrates a shift from bilateral consultations toward structured integration within EU digital resilience frameworks. Notably, the involvement of EEAS and EUISS signals the securitisation of digital policy, positioning Ukraine not only as a recipient of technical support but as a co-architect of regional cyber stability. These developments underscore the strategic importance of cybersecurity in the broader architecture of European security. The institutional deepening of cybersecurity cooperation is summarised in Table 18.1, which traces key milestones from bilateral dialogues to strategic investment planning.

Table 18.1

EU–Ukraine Cybersecurity Cooperation Milestones*

Year	Initiative	Lead Institution
2022	ENISA–Ukraine Cyber Dialogue	ENISA
2023	Joint Threat Intelligence Exchange	EEAS
2024	Cyber Resilience Framework Alignment	EUISS
2025	Strategic Cybersecurity Investment Plan	European Commission

**Source: compiled by author based on [4,7,12]*

The progression from ENISA-led dialogues to European Commission-led investment plans illustrates Ukraine's transition from technical recipient to strategic co-architect in EU digital resilience.

Ukraine's civil protection authorities have demonstrated operational resilience and solidarity, including dispatching aid to Türkiye following the February 2023 earthquakes. These actions reinforce Ukraine's credibility as a partner in European humanitarian and disaster response systems.

Strategic foresight: EU–Ukraine 2035 scenarios

The European Parliamentary Research Service's foresight study *EU–Ukraine 2035* outlines four plausible scenarios for the future of EU–Ukraine relations, based on two axes: the outcome of the Ukraine–Russia conflict and the depth of EU–Ukraine integration [5, p. 7].

Fair Stability: Ukraine regains full territorial control, joins the EU and NATO, and co-shapes a cooperative European security order. Defence and digital integration accelerate, and Ukraine becomes a net contributor to EU strategic autonomy.

Cold War II: The conflict remains frozen, with partial integration into EU structures. Ukraine becomes a frontline state in a bipolar world, with limited institutional convergence.

Frozen Conflict: Negotiated trade-offs lead to Ukrainian neutrality and a stagnant accession process. EU support continues, but strategic alignment weakens.

Devastated Europe: Escalation leads to NATO involvement and a fragmented EU. Ukraine remains resilient but isolated, with limited integration and high security volatility.

The economic dimension of Ukraine's integration into the European security architecture is reflected in the evolving structure of bilateral trade. Table 18.2 illustrates the dynamics of EU–Ukraine trade volumes across three strategic sectors - agriculture, energy, and ICT/cybersecurity - between 2020 and 2025. The data reveal a steady upward trend, with particularly pronounced growth in the energy and ICT sectors. This expansion corresponds to Ukraine's alignment with EU digital and energy frameworks, including grid synchronisation and cybersecurity cooperation. The projected figures for 2025 underscore Ukraine's increasing relevance as a strategic partner in the EU's economic and technological landscape. As shown in Table 4.1, Ukraine's trade with the EU has expanded steadily across strategic sectors. The ICT & Cyber category, in particular, demonstrates a compound

annual growth rate exceeding 20%, reflecting Ukraine’s integration into EU digital supply chains.

These figures underscore the economic dimension of Ukraine’s strategic relevance, with trade growth aligning closely with regulatory convergence and infrastructure upgrades supported by EU investment frameworks.

Table 18.2

EU–Ukraine Trade Volume by Sector, 2020–2025 (in million EUR)*

Sector	2020	2021	2022	2023	2024	2025
Agriculture	3,210	3,480	3,750	4,020	4,300	4,580
Energy	2,100	2,450	2,800	3,200	3,600	3,950
ICT & Cyber	1,050	1,300	1,600	1,900	2,250	2,600

**Source: compiled by the author based on [6,11,15]*

Building on current integration trends and strategic foresight literature, the following scenarios – adapted from the European Parliamentary Research Service (EPRS, 2024) – outline plausible trajectories for EU–Ukraine relations by 2035. These scenarios are structured along two analytical axes: the outcome of the Ukraine–Russia conflict and the depth of institutional integration with the European Union. Together, they offer a framework for anticipatory governance, risk assessment, and long-term policy planning.

These scenarios offer a framework for policy planning, risk assessment, and institutional design. They underscore the importance of flexible, scalable cooperation mechanisms that can adapt to geopolitical shifts.

Taken together, these scenarios underscore the strategic uncertainty surrounding Ukraine’s integration trajectory, while also highlighting the structural factors that enable resilience and adaptability. The empirical trends presented in Tables 4.1 and 4.2 suggest that Ukraine’s institutional convergence and sectoral growth are already shaping the contours of European security. Whether through full accession or functional alignment, Ukraine’s role in the EU’s future architecture will depend not only on geopolitical outcomes but on sustained regulatory, infrastructural, and digital cooperation.

Policy recommendations for deepening integration

Based on current trends and foresight analysis, the following policy recommendations are proposed to strengthen Ukraine’s role in European security.

Institutionalise defence cooperation through permanent joint procurement mechanisms, shared R&D platforms, and integration into the European Defence Fund.

Expand civil protection collaboration by establishing joint training centres, interoperable response protocols, and shared stockpiles of emergency equipment.

Accelerate digital convergence via mutual recognition of cybersecurity certifications, cross-border data governance frameworks, and joint AI ethics standards.

Support regional infrastructure resilience through co-financed projects under the Connecting Europe Facility and TEN-T, prioritising border regions and multimodal corridors.

Enhance strategic foresight capacity by embedding scenario planning and horizon scanning into EU–Ukraine policy dialogues, enabling proactive risk mitigation and adaptive governance.

These scenarios not only illustrate divergent geopolitical outcomes but also inform the design of flexible policy instruments. The recommendations in Section 4.4 respond to these foresight trajectories by proposing scalable, resilient mechanisms for defence, civil protection, and digital governance.

These recommendations aim to consolidate Ukraine’s position as a co-architect of European resilience, moving beyond reactive support toward structured, long-term integration.

Conclusion

This chapter has examined Ukraine’s evolving role in the European security architecture through the interlinked dimensions of geopolitical alignment, economic integration, digital resilience, and strategic foresight. By reframing Ukraine not as a peripheral actor but as a functional contributor to European stability, the analysis has addressed the central scientific problem: how Ukraine’s institutional convergence and infrastructural modernisation enhance the EU’s strategic autonomy and multidimensional resilience.

Empirical evidence has demonstrated Ukraine’s active participation in energy diversification, trade networks, and digital governance. Its alignment with EU regulatory frameworks – ranging from the Third Energy Package and DCFTA to GDPR and NIS2 – illustrates a deliberate and structured integration process. Ukraine’s contributions to civil protection, cybersecurity,

and critical infrastructure modernisation further reinforce its credibility as a partner in European resilience-building.

Looking ahead, Ukraine's strategic relevance is set to deepen. Continued reforms in public administration, defence cooperation, and digital infrastructure will strengthen reciprocal trust and institutional compatibility. Scenario modelling suggests that Ukraine's trajectory will be shaped not only by geopolitical outcomes but by its capacity to co-create shared governance frameworks and contribute to regional foresight.

In sum, Ukraine should be viewed not merely as a beneficiary of European security systems, but as a co-architect of their evolution. Its integration into the EU's economic, digital, and strategic domains reflects a broader transformation in the nature of European security - one that is collaborative, adaptive, and grounded in mutual resilience.

References

1. Ćwiek-Karpowicz, J. (2021). European security and neighbourhood dynamics. Warsaw: Polish Institute of International Affairs (PISM). 212 p.
2. Deltour, L. (2020). The EU and Ukraine: A partnership for resilience. *Journal of Common Market Studies*. Vol. 58, No. 2. P. 205–222.
3. Dragneva, R. (2023). Normative convergence and institutional trust in EU–Ukraine relations. *Europe-Asia Studies*. Vol. 75, No. 5. P. 889–896.
4. European External Action Service. EU–Ukraine cyber dialogue: Third round summary. Brussels: EEAS, 2024. 8 p.
5. European Union Agency for Cybersecurity. Enhanced EU–Ukraine cooperation in cybersecurity. Heraklion: ENISA, 2023. 15 p.
6. European Network of Transmission System Operators for Electricity. Ukraine's synchronisation with the Continental European grid: Technical report. Brussels: ENTSO-E, 2024. 54 p.
7. EU Institute for Security Studies. Strategic foresight report on Europe's security architecture. Paris: EUISS, 2024. 42 p.
8. European Commission. Ukraine and the EU: Key economic trends 2022–2024. Luxembourg: Publications Office of the European Union, 2023. 36 p.
9. European Commission. EU Civil Protection Mechanism: Ukraine response summary / Directorate-General for European Civil Protection and Humanitarian Aid Operations (DG ECHO). Brussels: EC, 2024. 12 p.

10. European Commission. Ukraine investment framework: Strategic orientations and implementation guidelines / Directorate-General for Neighbourhood and Enlargement Negotiations (DG NEAR). Brussels: EC, 2025. 28 p.
11. European Parliamentary Research Service. EU–Ukraine 2035: Strategic foresight scenarios. Brussels: EPRS, 2024. 30 p.
12. Havlik, P. (2023). Ukraine in European supply chains. Vienna: The Vienna Institute for International Economic Studies (wiiw). 40 p.
13. Kovalchuk, Y., Serdiuk, V. (2022). Digital security and cyber integration in Ukraine–EU relations. *Information & Security*. Vol. 50, No. 3. P. 172–182.
14. Mankoff, J. (2022) Empowered Europe: The strategic relevance of Ukraine. Washington, DC: Center for Strategic and International Studies (CSIS). 60 p.
15. McGowan, F. (2020). Security and the Energy Union: The role of Eastern Europe. London: Palgrave Macmillan. 288 p.
16. Palko, A. (2021). Transport corridors and regional integration in Eastern Europe. Cham: Springer. 210 p.

Chapter 19
***Competitiveness of corporate associations of enterprises in
the system of Ukraine's cross-border integration
into the EU***
(O. Hutsaliuk, Iu. Bondar)

The processes of cross-border integration that are intensively unfolding in the context of Ukraine's gradual European integration are imposing new requirements on the national economy and its actors, in particular on corporate associations of enterprises. The formation of a single economic space with the countries of the European Union highlights the need to enhance the competitiveness of Ukrainian business structures and their ability to operate effectively within the highly competitive and institutionally complex environment of the EU.

Corporate associations in the form of clusters, holdings, industrial and financial groups, and other integrated structures – serve as an important instrument for strengthening the positions of enterprises in both domestic and foreign markets. Their significance increases in conditions that require the pooling of resources, innovative potential, managerial competencies, and strategic development vision within the framework of cross-border interaction. However, existing models of corporate cooperation in Ukraine often fail to meet the requirements of the modern knowledge-based economy, European business standards, and the challenges associated with market openness, technological shifts, and the growing intensity of global competition.

The relevance of this study is determined by the need for an in-depth analysis of the factors influencing the competitiveness of corporate associations of enterprises in the context of cross-border integration, as

well as the identification of barriers and the adaptive potential of such structures to EU standards. Particular attention should be paid to examining the institutional environment in which corporate associations operate and to developing strategic approaches aimed at enhancing their efficiency and resilience amid the transformation of economic relations.

The aim is to conduct a comprehensive study of the specific features of forming competitive advantages of corporate associations in the context of cross-border integration, taking into account the challenges of Ukraine's European integration trajectory, as well as to develop practical recommendations for strengthening their role in the processes of economic modernization and regional development.

19.1. Integration paradigm of competitiveness formation of cross-border cooperation entities

In the current context of globalization and active integration processes in Europe, the issue of the competitiveness of corporate associations of enterprises is gaining particular importance for Ukraine. The prospect of full integration into the single European economic space requires national businesses not only to comply with EU standards but also to demonstrate the ability to compete effectively in open markets. It is precisely corporate associations of enterprises – such as holdings, consortia, associations, and clusters – that serve as institutional forms enabling the concentration of resources, optimization of management processes, and strengthening of positions in both domestic and international markets.

Ukraine's cross-border integration with the European Union creates new opportunities for the development of corporate structures. It entails expanded access to financial instruments, joint innovation programs, cross-border infrastructure, and logistics. At the same time, integration processes pose a number of challenges, including the need to harmonize legal frameworks and adapt to European standards of management, environmental requirements, and social responsibility. In this context, the competitiveness of corporate associations becomes a determining factor that allows them not

only to maintain their positions in the national market but also to take a worthy place among the leading European players.

Research into this issue is important in light of Ukraine's strategic priorities aimed at strengthening integration interaction with the European Union, shaping a modern economic system, and creating conditions for sustainable development. An analysis of the mechanisms for enhancing the competitiveness of corporate associations makes it possible to identify the most effective integration tools, among which innovative technologies, international partnerships, the development of cluster initiatives, and the active attraction of investment occupy a special place.

Issues related to ensuring the competitiveness of business entities have remained highly relevant for a considerable period of time. Their relevance is not обусловлена by a lack of developments or insufficient research in the field of enterprise competitiveness management. At present, there exists a substantial body of research devoted to the theoretical identification of the concepts of 'competition' and 'competitiveness', as reflected in the works of such economists as L. I. Piddubna [14], C. K. Prahalad [18], and Yu. B. Ivanov [9].

Researchers have also addressed the issues of assessing the level of enterprise competitiveness (outlined in the studies of V. A. Pavlov [13] and O. H. Yankovyi with co-authors [10]), the formation of competitiveness management frameworks (presented in the works of, for example, A. A. Pylypenko with co-authors [16], M. V. Malchyk [11], and A. E. Voronkova [3]), as well as the development of competitive strategies (with the classical example being the works of M. Porter [15]), among others.

At the same time, the high turbulence of the business environment, the emergence of breakthrough innovations alongside the overall intensification of innovative activity, and the appearance of new forms of economic activity and organization of technological processes give rise to new aspects that require adaptation of the existing theoretical and methodological framework across all sectors of the economy. This precisely underpins the sustained relevance of issues related to the formation and management of competitiveness of business entities. One such factor is the emergence of integrative forms of interaction between enterprises, within which a phenomenon of combining competition and cooperation arises (this phenomenon is described in the works of C. K. Prahalad [18] and N. I. Chukhrai [20]).

The influence of the integrative foundation on the logic, dynamics, and organization of competitiveness management has been examined in the works of V. M. Horbatov [5], who investigated the impact of the type of integrative structure and its life cycle stage on the level of competitiveness. In turn, the author of the present study [6] also considered issues related to analyzing the impact of synergy arising from integrative interaction on the parameters of an integration strategy aimed at enhancing the competitiveness of corporate enterprises.

At the same time, in all the aforementioned studies [5–6; 15], the interaction between integration and competitiveness does not reflect consideration of a relatively new research direction for domestic scientific thought, namely the development of cross-border cooperation. This is despite the fact that the study of the organizational features of cross-border cooperation has been undertaken by such scholars as N. Mikula [12], who developed a methodological framework for the formation and evaluation of the effectiveness of a cross-border region; I. V. Artiomova with co-authors [19], who highlighted current issues of cross-border cooperation and defined its role in state-level integration processes; V. S. Kravtsiv [17], who examined the forms and trends of Euroregional cooperation development; L. M. Hazuda [4], who analyzed the specific features of foreign economic activity carried out by entities of cross-border cooperation; as well as many others.

It should be noted that in the above-mentioned studies, primary attention was focused on establishing cross-border cooperation or organizing interaction among its participants within value creation chains. It is quite evident that the formation of such chains is grounded in the phenomenon of integration. At the same time, the cited authors [17; 19] did not examine integration in relation to assessing the competitive advantages gained by participants in integration-based interaction. Moreover, in most cases integration was studied solely in the context of shaping the relevant frameworks of state regulation within the provisions of the Law of Ukraine ‘On Cross-Border Cooperation’ (in particular, concerning the establishment of cross-border cooperation bodies and the development and implementation of relevant state programs). In view of this, the purpose of this study is to assess the possibility of obtaining additional competitive advantages through integration and to examine the specifics of their realization in cross-border markets.

The importance of studying the integration basis of competitiveness of cross-border cooperation entities is also confirmed empirically. According to data presented in [17, pp. 9–11], 12 industrial parks are registered in Ukraine, 10 euroregions operate, cross-border trade is developing, and several cross-border clusters have been established (for example, the ‘Polish–Belarusian–Ukrainian’ cluster and the ‘Cross-Border Innovation Cluster’). Indicative allocations under the land border programs ‘Hungary–Slovakia–Romania–Ukraine’ and ‘Romania–Moldova–Ukraine’ for the period 2020–2024 amounted to EUR 68.6 million and EUR 126.7 million respectively; the Black Sea Basin maritime program accounted for EUR 17.3 million [12, pp. 90–91]. At the same time, national business entities participated in less than 20% of the cross-border cooperation programs of the European Neighbourhood and Partnership Instrument (ENPI) [17, p. 11], which indicates the existence of significant potential for expanding integration-based interaction.

In this regard, the position of Z. S. Varnalii [2, p. 687] concerning the presence of a number of positive effects resulting from the expansion of cross-border cooperation should be supported. The main benefits include growth in the number of cooperation agreements, development of interaction infrastructure, improvement of knowledge management and implementation of joint research activities, enhancement of the capacity to address common or similar problems, harmonization of strategic interaction institutions among participants of cross-border clusters, increased investment and intensified innovation activity, as well as opportunities for cooperation in the implementation of infrastructure projects, among others. As can be seen, most of the listed prerequisites for the expansion of cross-border cooperation are associated both with strengthening the competitive potential of individual economic entities and with the development of their strategic interaction with other actors. In this context, emphasis is placed on the necessity of developing and disseminating an integration paradigm for shaping the competitiveness of cross-border cooperation entities (participants).

It should be emphasized that the approach envisages correlating various factors contributing to the emergence of competitive advantages with the incentives driving the spread of integration processes (at the first, initial level of the hierarchy – defined as the level of ‘creating a basis for assessing the feasibility of integration’). Based on a detailed characterization of the author’s interpretation of such correlation, presented in [6], the relevance of identifying competitive advantages derived directly from cross-border

integration interaction is substantiated. This approach partially overlaps with studies in the field of ensuring international competitiveness, such as those in [14–15], yet it is characterized by a substantially different nature.

The identification of such competitive advantages is envisaged at the second level of the overall hierarchy, referred to as the ‘impact of cross-border cooperation’. Within the components of this level, an interesting proposition by N. Mikula [12, pp. 28–30] regarding the existence of centrifugal trends in regional development is employed. This implies that the highest level of development within a country is typically characteristic of central regions, with a gradual decline toward peripheral areas. Accordingly, cross-border cooperation serves as a tool for altering the direction of this trend. Indeed, entities located in border regions can gain access to additional competitive advantages through integration, which fully corresponds to the motives underlying the initiation of integration-based interaction.

Differences in the level of development of cross-border regions constitute a basis for economic entities to adopt best business practices, which ultimately provides them with additional competitive advantages. In this context, the creation of such advantages may be based either on an integration framework or implemented outside the scope of integration interaction. This differentiation of opportunities for creating competitive advantages has determined the hierarchy of the subsequent, third, level of the hierarchy. This level (the level of the ‘nature of manifestation of competitive advantages’) is revealed as the identification of the manifestation of integration incentives on the factors of competitiveness of participants in cross-border cooperation (as a reflection of the impact of these incentives on the availability and strength of the manifestation of competitiveness factors). A distinctive feature of this level is the consideration of the possibility of losing competitive advantages or market positions after the implementation of integration processes. Indeed, although integration may lead to negative effects and reverse synergy, most researchers tend to consider it solely as a positive phenomenon.

When discussing the nature of competitive advantages, it is essential to pay attention to the possibilities of their realization, which are determined by the regulations of agreements governing cross-border cooperation. Indeed, the forms of cross-border cooperation chosen in a particular region, to a greater or lesser extent, influence the behavior of enterprises.

V. S. Kravtsiv [17, pp. 19–22] analyzes an expert survey of representatives of local authorities who regulate various aspects of cross-border cooperation (91 respondents from 16 regions were surveyed).

According to the results of this study, the most effective forms were interregional agreements (17.8% of respondents identified this form as the most effective in terms of ensuring regional development), cross-border projects (24% of respondents supported this form of development), and cross-border partnerships (indicated in the responses of 15.6% of respondents). These results confirm the significance of integration interaction among individual economic entities as a basis for the emergence of additional competitive advantages.

Furthermore, the parameters of the business model of corporate integration associations (CIAs) are directly dependent on the form of organization of cross-border cooperation and the form of regulation of such cooperation. Moreover, depending on the chosen basis for creating advantages, the organizational and structural form of the cross-border cooperation entity will also be determined. In view of this, the next, fifth, level of the proposed hierarchical model is introduced. This level defines the organizational form of establishing a corporate integration association. For the purposes of this study, an aggregated list of CIAs is used, classified according to the degree of rigidity and strength of restrictions on the activities of participants in integration interaction (classification based on the 'softness' and 'rigidity' of integration).

Having determined the form of establishment of the KIO, the next level defines the approach to competitive positioning. At the sixth level of the hierarchy, one of the fairly common (generally accepted) approaches to describing such positioning is applied. At the same time, it is necessary to emphasize certain differences in the substantive content of this hierarchical level. These differences, first, are based on the characteristics of cross-border cooperation identified in studies [4; 12; 17; 19]. In this context, the increase in the competitiveness of cross-border cooperation actors is understood to be grounded in the creation of specific advantages at the regional level. Accordingly, competitive positioning is carried out to a greater extent not in relation to individual competitors but within the positioning of a particular border region (although individual actors independently develop their own competitive strategies).

Thus, second, it is precisely under the conditions of cross-border space, at the fourth level of the hierarchy – represented by clusters or partnerships – that the 'coopetition' relationships discussed in [18] become particularly intensified. Their existence is declared as one of the possible forms of competitive behavior (presented as an element of 'Development of

competitive–cooperative interaction with market segment allocation’), which manifests itself within the border regions of different countries.

A distinctive feature of the authors’ proposals in this case is the anticipation of mutual enrichment of individual components of these strategies. Such enrichment of strategies, as well as the use of the hierarchy as a whole, can be implemented at different levels of the national economic system. At the macro- and meso-levels, the value lies in the possibility of a more substantiated choice of organizational forms for managing cross-border interaction, both in terms of their alignment with the development of key competencies of cross-border cooperation actors and in terms of creating an environment for extracting systemic effects from interaction.

Therefore, the integrative paradigm for forming the competitiveness of cross-border cooperation actors is based on the combination of resource potential, managerial innovations, and the synergy of partnership relations between Ukrainian and foreign enterprises. It enables not only an increase in the efficiency of individual actors but also ensures the sustainable development of corporate alliances within the European economic space. The formation of competitiveness in the integrative dimension contributes to the intensification of investment, the expansion of sales markets, and the implementation of modern technologies, which, in turn, strengthens Ukraine’s position in cross-border cooperation and brings it closer to full integration with the EU.

19.2. Justification of the parameters of competitive positioning of cross-border cooperation entities

In the current conditions of globalization and the intensification of European integration processes in Ukraine, the issue of enhancing the competitiveness of corporate associations of enterprises operating in the field of cross-border cooperation becomes particularly relevant. Entry into international markets requires not only the improvement of internal business processes but also the formation of a sustainable model of competitive positioning that takes into account the specifics of the European market environment, legal regulations, and the economic standards of the European Union. In this context, corporate associations of enterprises serve as an important instrument for Ukraine’s integration into the European economic space, as they enable resource consolidation, risk reduction, and the implementation of large-scale innovative projects.

Justification of the Parameters of Competitive Positioning of Cross-Border Cooperation Entities is a key task of strategic management, as it ensures the identification of the strengths and weaknesses of enterprises, the recognition of opportunities and threats in external markets, and the formation of an effective marketing policy. In particular, this involves selecting optimal differentiation, pricing, and innovation strategies, which enable Ukrainian companies to successfully compete with European partners and integrate into international value chains.

Researching the parameters of competitive positioning within the framework of Ukraine's cross-border integration with the EU has both theoretical and practical significance. It contributes to developing recommendations for businesses to enhance cooperation efficiency, design joint investment projects, and attract foreign partners, which ultimately strengthens the country's economic resilience and accelerates its integration into the European space.

At the micro level, it should be noted that an individual economic entity in a border region can have a strategic development profile formed in accordance with the rules for participating in cross-border cooperation within the integration framework. As can be seen in Table 1.1, the formation of the elements of this profile occurs conceptually as a pairwise correlation of individual levels of the hierarchy developed by the author. For example, the competitive advantage options presented in Table 1.1 are determined by correlating the factors generating competitive advantages at the first level of the hierarchy with the incentives for spreading integration processes. Another example is the presented list of integration growth accelerators, which is based on matching the nature of competitive advantages with the forms of cross-border cooperation.

The main purpose of introducing the profile presented in Table 1.1 is to identify the characteristics of the competitive behavior of a specific participant in cross-border interactions. As can be seen from Table 19.1, the elements of the developed profile are distributed across the lower-level hierarchy of integration and competitive strategy. In practical terms, the implementation of the author's proposals is based on the distribution of elements of the proposed strategic profile by types of competitive behavior of economic agents, as indicated in Table 19.2, which were defined at the penultimate level of the hierarchy.

Table 19.1

Strategic profile for building the competitiveness of cross-border cooperation entities*

Profile element ({P})	Variants of implementation of profile elements within the economic activities of a cross-border cooperation entity				
Components of a Competitive Strategy for a Participant in Cross-Border Cooperation					
P1 Basic Competitive Strategy (according to M. Porter [15])	P1.1 Cost Leadership Strategy	P1.2 Broad Differentiation Strategy	P1.3 Focused Low-Cost Strategy	P1.4 Focused Differentiation Strategy	P1.5 Best-Cost Strategy / Optimal-Cost Strategy
P2. Basic Development Strategy	P2.1 Stability Support Strategy	P2.2 Development Strategy (Limited or Integrative)			P2.3 Retrenchment Strategy
P3 Competitive Rivalry Activity	P3.1 Offensive (Attack) Strategy	P3.2 Defensive Strategy or Market Position Retention Strategy		P3.3 Indifferent (Avoidance) Strategy	P3.4 Withdrawal Strategy
Priorities for Ensuring Competitiveness within the Framework of Integration Interaction					
P4 Marketing and Market Positioning	P4.1 Attracting a New Brand	P4.2 Expanding Reputation Assets	P4.3 Consolidation of Marketing Expenditures	P4.4 Increasing Market Power	P4.5 Integrated Marketing Communications
P5 Formation of the logistics system and distribution	P5.1 Integration of client networks	P5.2 Expansion of SCM networks and logistics interaction	P5.3 Development of distribution channels and service		P5.4 Demonstration of combinatorial uniqueness
P6 Technology and Methods of Management	P6.1 Increasing the adoption of innovative work methods		P6.2 Improving quality through redistribution of product control		P6.3 Access to new equipment and emerging technologies
Profile Element ({P})	Options for Implementing Profile Elements within the Economic Activities of a Cross-Border Cooperation Entity				
P7 Expenses and Access to Resources	P7.1 Formation of a resource combination that is difficult to replicate		P7.2 Enhancement of all types of potential	P7.3 Maximization of resource potential	P7.4 Dissemination of knowledge about resource zones
P8 Organization of Management Processes	P8.1 Selection of the Most Effective Forms of Interaction		P8.2 Minimization of Transaction Costs	P8.3 Development of Corporate Culture	P8.4 Selection of Optimal Management and Motivation Methods
P9 Optimization of Architectural Representation	P9.1 Creation of an Institutional Interaction Environment		P9.2 Consolidation of Scarce Resources and Their Processing Technologies	P9.3 Optimization of Organizational Structure and Size of the KIO	P9.4 Selection of the Most Efficient Forms of Activity
P10 Information Support and Knowledge Exchange	P10.1 Mobility in acquiring innovations and knowledge	P10.2 Intensification of information exchange	P10.3 Acceleration of knowledge diffusion	P10.4 Overcoming institutional traps	P10.5 Increasing the value of consolidated information

Table 19.1 (continued)

Components of the Integration Strategy of a Participant in Cross-Border Cooperation					
P11 Basic Strategy	P11.1 External Transformation (Expansion or Reduction of CIO)	P11.2 Business Cooperation (Integrated Behavior)	P11.3 Operational Consolidation and Formation of Interaction Networks	P11.4 Consolidated Protection of Existing Market Positions	
P12 Choice of the Form of Creating a Corporate Industrial Organization (CIO)		P12.1 Separate Corporate Enterprise	P12.2 Rigid Integrated Holding	P12.3 Conglomerate Based on Property Relations	P12.4 Flexible Integration Association
P13 Accelerator of Integration Growth	P13.1 Institutional and Cultural Renewal	P13.2 Expansion of Market Power	P13.3 Economies of Scale	P13.4 Leveraging Network Effects	P13.5 Protection and Capture of Positions

**Source: compiled by the authors based on [1–2; 7; 17].*

The approach to competitive positioning described in Table 1.2 is based on the initial decision of an economic agent regarding engagement in integration or cooperative interaction. The author's hypothesis, in this case, consists in determining the extent of such interaction and regulating its influence on the parameters of the agent's competitive behavior.

Thus, the author's proposals focus on the development of a methodology for identifying and enhancing areas of competitive advantage that emerge during cross-border interactions between individual economic entities. The justification of the parameters for competitive positioning of cross-border cooperation participants demonstrates the multidimensional nature of the strategic profile, encompassing fundamental competition and development strategies, competitive activity, marketing positioning, logistics system formation, as well as organizational and managerial aspects. The presented table allows correlating the recommended profile elements with specific types of competitive positioning (CP1–CP4), forming a basis for selecting the most effective trajectory for the development of cross-border partnership entities.

This approach provides a systemic view of which strategic tools should be prioritized in the context of Ukraine's integration processes with the EU. At the same time, the variability of parameters within different competitive positioning models allows for adaptation of strategies to specific market conditions, resource availability, and institutional environment. Consequently, the alignment of core strategies, organizational mechanisms, and innovation priorities creates a foundation for building competitive corporate associations in the cross-border space.

Table 19.2

Justification of the Parameters for Competitive Positioning of Cross-Border Cooperation Entities*

Element of Strategic Profile ({P})	Recommended Profile Elements in Terms of the Specified Type of Competitive Positioning ({CP})			
	KP1	KП2	KP3	KP4
P1. Basic Competitive Strategy	P1.1, P1.3	P1.2, P1.4	P1.3, P1.4	P1.2, P1.5
P2. Basic Development Strategy	P2.2	P2.1–P2.3	P2.1, P2.2	P2.2
P3. Competitive Activity / Intensity of Competition	P3.1	P 3.2–P 3.4	P 3.2, P3.3	P 3.2, P 3.3
P4. Marketing and Market Positioning	P4.1, P4.2	P4.2–P4.4	P4.2, P4.3	P4.2, P4.5
P5. Formation of Logistics System and Distribution	P5.3	P5.2, P5.3	P5.4	P5.1, P5.2
P6. Technology and Methods of Operations	P6.2	P6. –P6.3	P6.3	P6.1 – P6.3
P7. Costs and Access to Resources	P7.2, P7.3	P7.2, P7.4	P7.1	P7.4
P8. Organization of Management Processes	P8.4	P8.1, P8.3	P8.3, P8.4	P8.1, P8.2
P9. Optimization of Architectural Representation	P9.2, P9.4	P9.3	P9.2, P9.4	P9.1
P10. Information Support and Knowledge Exchange	P10.1, P10.5	P10.4	P10.1	P10.2, P10.3
P11. Core Strategy	P11.1	P11.1	P11.4	P11.3, P11.2
P12. Selection of the Form of Corporate Association Formation	П12.1, П12.3	П12.1, П12.3	П12.1	П12.4
P13. Accelerator of Integrative Growth	П13.5	П13.1	П13.2, П13.5	П13.3, П13.4

**Source: compiled by the authors based on [14; 16–17; 19].*

The competitiveness of corporate associations of enterprises within Ukraine's cross-border integration with the EU is a significant factor for economic development and enhancing the country's position in international markets. In the current context of globalization and intensified interregional interaction, corporate associations (consortia, clusters, associations) are becoming key instruments that enable enterprises to more effectively adapt to European market requirements, implement innovations, improve management standards, and attract investments.

Cross-border integration offers opportunities for creating joint production chains, developing export potential, and strengthening the positions of Ukrainian enterprises in the competitive environment of the EU. The exchange of experience, technologies, and management practices with European partners is also crucial, as it allows corporate associations to reach a qualitatively new level of development.

At the same time, the competitiveness of Ukrainian corporate structures depends on several factors: state support for integration processes, the institutional capacity of enterprises, access to financial resources, the ability to engage in innovative activities, and the preparation of qualified personnel. Particularly important are mechanisms for harmonizing standards and regulations with European legislation, as these provide access to the common market.

Therefore, enhancing the competitiveness of corporate associations within Ukraine's cross-border integration with the EU is possible through the combination of strategic business and state interests, active participation in international cooperative projects, and consistent implementation of economic integration policies. This will allow Ukrainian enterprises not only to maintain their positions in the domestic market but also to secure a worthy place in the European economic space.

References

1. Bondar, Iu. A., Lehinkova, N. I., Fabryka, I. V. (2022). Analysis of Methods for Determining the Competitiveness Level of Enterprise Products. *Bulletin of Postgraduate Education, Series "Social and Behavioral Sciences."* 22 (50), pp. 161–178. [https://doi.org/10.32405/2522-9931-2022-22\(51\)-161-178](https://doi.org/10.32405/2522-9931-2022-22(51)-161-178)
2. State Regional Policy of Ukraine: Features and Strategic Priorities: Monograph / Ed. by Z. S. Varnalia. Kyiv, 2007. 720 p.
3. Voronkova, A. E. (2008). Managerial Decisions in Ensuring Enterprise Competitiveness: Organizational Aspect: Monograph/A.E. Voronkova, N. G. Kalyuzhna, V. I. Otenko. Kharkiv: INJEK Publishing, 427p.
4. Hazuda, L. M., Rubin, M. A. (2015). Implementation of Joint Cross-Border Cooperation Projects. Uzhhorod: FOP Sabov A. M. Publishing, 276p.

5. Horbatov, V. M. Competitiveness and Development Cycles of Integrated Business Structures: Monograph. Kharkiv: INJEK Publishing, 2006. 592 p.

6. Hutsaliuk, O.M. Integration Basis for Managing Competitive Positioning of Corporate Enterprises. *Business Navigator*, 2017, Issue 4-1 (43), pp. 136–142.

7. Hutsaliuk, O. M., Bondar, Iu. A., Kravchenko, M. S., Fediuk, B. O. (2025). Corporate Management of Strategic Communications and Reputational Risks in Small and Medium Enterprises: Ukraine VS EU. *Bulletin of Economic Science of Ukraine*, 1 (48), pp. 95–103. [https://doi.org/10.37405/1729-7206.2025.1\(48\).95-103](https://doi.org/10.37405/1729-7206.2025.1(48).95-103)

8. Hutsaliuk, O. M., Bondar, Iu. A., Zaichenko, V. V. (2025). Organizational Imperatives for Ensuring Economic Security of Corporate-Integrated Enterprises and Associations in the Hospitality Industry. *Strategy for the Recovery of Deoccupied Territories of Ukraine: Challenges of Post-Conflict Development and Ways to Overcome Them*: Collective Monograph. Ivano-Frankivsk: KDU, pp. 566–581. Available at: <https://zenodo.org/records/15189585>

9. Ivanov, Yu. B. (2004). Enterprise Competitiveness: Evaluation, Diagnostics, Strategies: Scientific Publication by Collective of Authors. Kharkiv: KhNEU Publishing, 256 p.

10. Enterprise Competitiveness: Assessment and Directions for Improvement: Monograph / Ed. by O.G. Yankovyi. Odesa: Atlant, 2013. 470p.

11. Malchyk, M.V. (2010). Reflexive Management of Industrial Enterprise Competitiveness: Monograph. Donetsk–Rivne: PP Lapsiuk V.A., 216 p.

12. Mikula, N. A., Zasadko, V. V. (2014). Ukraine's Cross-Border Cooperation in the Context of European Integration: Monograph. Kyiv: NISD, 316 p.

13. Pavlova, V. A. (2006). Enterprise Competitiveness: Assessment and Strategy of Provision. Dnipro: DUEP Publishing, 276 p.

14. Piddubna, L. I. (2011). International Competitiveness of Enterprises: Theory and Mechanisms of Provision. Kharkiv: INJEK Publishing, 400 p.

15. Porter, M. (1998). Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press, Illustrated Edition, 397 p.

16. Pylypenko, A. A., Fartushniak, O. V., Pasichnyk, I. Yu. (2017). Competitiveness of Industrial Enterprise Products: Management Organization and Marketing Support: Monograph. Kharkiv: FOP Liburkina L.M., 280 p.

17. Development of Cross-Border Cooperation: Scientific-Analytical Report / Ed. by V.S. Kravtsiv. Lviv: NAS of Ukraine, 2016. 125 p.

18. Prahalad, C. K., Ramaswamy, V. (2005). The Future of Competition: Co-Creating Unique Value with Customers [Translated from English by M. Stavytsky]. Kyiv: Oleksiy Kapust Publishing, 258 p.

19. Cross-Border Cooperation of Ukraine: Status, Problems, Prospects: Monograph / Ed. by I.V. Artyomov. Uzhhorod: MPP "Grazhda", 2012. 520p.

20. Chukhrai, N. I. (2011). Cooperation as a Strategy for Enterprise Functioning in the Innovation Market. *East-European Journal of Advanced Technologies*, 1 (5), pp. 20–22.

Chapter 20
***European security and Ukraine: the role of international
organizations in financial stability***
(R. Ivanova)

The 2022 Russian invasion of Ukraine has had far-reaching consequences on the European security architecture. The 21st century reality has indeed shifted after this invasion. States currently balance the interlinked dependencies of sovereignty, democracy, and financial management system governance. Ukraine is situated at the frontline of Europe's defense of democracy and acts as a monument to the struggle of democracy, as well as a battlefield of the fight for institutional cohesion, security integration, and global financial collaboration.

At the center of the confrontations surrounds the topic of financial stability. It serves as the backbone of a nation's endurance, policy freedom, and ability to manage crises rather than just an indicator of macro economy. For Ukraine, the war has brought unprecedented destruction to this infrastructural framework: imploding GDP, infrastructure damage, fiscal deficits, and inflationary pressures. It does not only undermine Ukraine's financial system, but the entire European security and economic architecture system.

The response from international organizations has been unprecedented in scope and significance. The European Union, the International Monetary Fund, the World Bank, and the European Bank for Reconstruction and Development (EBRD) have augmented their activities beyond the customary aid-facilitating frameworks. These institutions are now co-designing Ukraine's transformational institutional and legal reforms by integrating governance restructuring and pre-emptive Ukraine's European integration anchoring.

This paper investigates the role of international financial aid in structured legal frameworks, oversight systems, and conditional policies in contributing to national security policies. It traces the processes of legal alignment, digital modernization, and strategic resource mobilization as Ukraine's relations with international organizations evolved into a multilateral endeavor. This study, anchored in law and sociology, examines the how, the consequences, and the strategic outcomes of Ukraine's engagement with the European financial security architecture during its war and reconstruction efforts.

As the chapter demonstrates, financial stability emerges as a core concern within the broader framework of European security – not merely as a peripheral issue. The enduring existence of democratic nations facing an existential threat is bound to depend on the existence of strong, legitimate, and internationally integrated financial governance.

20.1. The role of economic stability in European security policy

The link between security issues and finances is growing in popularity in international legal studies, especially in Europe. Financial security is increasingly seen not just as an element of sustenance but rather a central component of statehood and defense. In the context of international law, the availability of economic sovereignty and equilibrium within the state's macrosystem is essential for the exercise of other functions of the state which are guaranteed as fundamental rights in international legal documents like the United Nations Charter and even by the regional legal documents like Treaty on the European Union.

In the case of Ukraine, the aggressor state has weaponized the finances of this country. The contraction of gross domestic product by over 30% in 2022. The destruction of central infrastructure together with an ever-increasing budget deficit highlights the fact that financial disruption is both a consequence and a tool of warfare. The prevailing conditions compelled the Ukrainian government to institute emergency monetary and fiscal policies like deficit monetization, domestic regulatory capture, external borrowing, and others – all of which limit self-governing control over fiscal policy.

Besides this, Ukraine's financial fragility puts Europe in a precarious position financially as it constitutes an entire system. Through trade, migration, and investment networks, any disruption in Ukraine's economy translates into greater socio-economic risk for the Eastern borders of the EU. As a result, from a legal-policy perspective, the EU has spatially located Ukraine's financial viability as stemming from its Common Foreign and Security Policy (CFSP) which integrates financial equilibrium with boundary control and democratic consolidation in the region.

The approach of comprehensive security, which is increasingly accepted in Europe legal systems, incorporates economic resilience traits of public finance systems, institutional governance, and transparent public procurement. Therefore, Ukraine's macro-financial governance reform poses as a challenge of domestic policy only if an EU sympathisant participates.

Equally important is the understanding of financial security as an aspect of hybrid resilience, promoted by NATO and the EU in the face of hybrid threats, such as disinformation, cyber, and economic warfare. Ukraine's case illustrates that the loopholes available in the financial system are some of the most potent weaknesses vulnerable to geopolitical aggression. Preventing financial institutions from hostile acquisitions, embezzlement, and capital drain is not only a fiscal issue but a matter of state defense.

From a legal perspective, Ukraine's financial law needs to further develop in the direction of European norms and security features simultaneously, resulting in hybrid financial-legal instruments that have both civilian and security purposes. This requires more collaboration between financial authorities and national security agencies, which pose issues of inter-institutional equilibrium and responsibility, needing sophisticated legal answers.

20.2. Ukraine: legal aspects of international financial aid

The legal framework available in the context of financial stabilization of Ukraine is structured from multilateral and bilateral frameworks which prescribe the modalities, terms, and supervision of the financial aid offered. Most important within this framework is the Ukraine Facility of the European Union, which is put in place for the period of 2023–2027 and is worth EUR 18 billion. It is managed under the system of EU law and memoranda of agreements with the Government of Ukraine that impose conditions on public administration reform, anti-corruption, and transparency of governance. This

set of conditions does two things at once: limits the misuse of public spending, as well as encourages Ukraine's legal and institutional frameworks to move towards those of the EU. As an example, the Ukraine Facility requires progression in areas such as budget transparency, compliance with EU competition law, and creation of independent regulators for financial markets. Not adhering to these conditions may lead to the suspension or diversion of funding – something already established in the EU's external financial instruments.

In the context of international financial law, conditionality clauses operate as enforcement tools to ensure compliance with the reform goals set by the parties involved. They exist in all IMF Stand-By Arrangements, as well as Extended Fund Facility agreements like the one Ukraine received in 2023, which included USD 15.6 billion EFF. These arrangements are grounded in the IMF Articles of Agreement and are interpreted with respect to principles of global economic governance focused on promoting sound fiscal policies and anti-crisis stability.

The qualifying nature of IMF contracts has drawn considerable attention from researchers. Although not legally enforceable international obligations in the traditional view, they remain 'soft law' guidelines with powerful coercive capacity because of their effect on market trust and the availability of further funding. In Ukraine, the IMF has played an important role in obliging legal change at the level of central bank autonomy, design of the fiscal rule, and financial sector oversight.

The World Bank functions through its Multi-Donor Trust Funds and the International Bank for Reconstruction and Development (IBRD) by using both grants and loans. The legal regime of these instruments under World Bank operational policies is equally shaped by a blend of donor custom seeking to align development aid with strategic development priorities. The European Bank for Reconstruction and Development (EBRD) under its charter and relevant host country agreements rounds out this system with financing and technical assistance projects aimed at private and public infrastructure.

From the viewpoint of a legal institution, one of the principal innovations is the creation of the Multi-agency Donor Coordination Platform for Ukraine. The platform is more than a space for information sharing; it is a legal entity with a formal purpose, regulations, and structures of responsibility. It serves as a coordinating body for bilateral and multilateral

donors, ensuring that funding is consolidated, congruent with national priorities, and is jointly monitored and assessed.

This emerging adaptative legal system highlights the adoption of a governance ‘framework’ which blends different systems of providing international aid to one country. Efforts have been made to study this multi-faceted problem of governance that is made of multiple systems and structured forms that is so complex and tangled together that it needs legal mutants, cross recognition, and interoperability. On the other hand, Ukraine is a perfect case study for this novel legal regime in the international financial system governance.

20.3. The modernization of institutions and the reforms of the law as steps towards financial integration

There is no way to categorize institutional changes as purely a technocratic exercise. In Ukraine it entails a legislative duty to pursue the Euro-Atlantic integration and European Union membership. There is a new referral system of acquiring legal acts to the capturing the essence of Ukraine's alignment with European requirements and its financial institutions which is based on an evolving body of laws, policies, and treaties. In the field of regulating the financial services, audit, public internal financial control, and anti-money laundering, Ukraine has received legislation due to Association Agreement with EU which has been effective since 2017.

Strengthening the governance and autonomy frameworks of the National Bank of Ukraine (NBU) features as one of the core components of institutional modernization. Considerable reforms aimed at increasing the legal independence of the NBU have been undertaken since 2015, including changes to its charter, reporting obligations, and appointments to the governing board. Based on the recommendations from the IMF and the EU, these measures seek to ensure that the central bank functions in accordance with the provisions of Article 130 of the Treaty on the Functioning of the European Union which requires complete autonomy of political control over monetary authorities.

Another area of attention is reforming public financial management (PFM). Ukraine's State Treasury reform and the establishment of a medium-term budgetary framework (MTBF) serve as cornerstone building blocks in the pursuit of fiscal transparency and discipline. These strategic efforts, under the guidance of the Public Financial Management Strategy 2022–2025, seek

to guarantee that government spending is strategically prioritized and that public funds are spent in a manner that reflects a results-driven approach. Legally, this process falls within the realms of newly adopted Budget Code amendments and PEFA (Public Expenditure and Financial Accountability) compliance.

Additionally, the modernization of tax and customs administrations is part of the tax institutional modernization strategy. The establishment of the Bureau of Economic Security of Ukraine BESU and the automation of customs processes via the Single Window system mark significant milestones in the fight against corruption and revenue mobilization. These tax administration strategies are not only internal focal points but also parts of the obligations Ukraine contracted within the scope of Deep and Comprehensive Free Trade Area DCFTA chapter of the Association Agreement which stipulates the alignment of Ukraine with the Union Customs Code and the EU VAT Directive.

Within these transformations, the importance of digital tools is vital. The digitization of fiscal functions such as electronic declarations of public servants, the automated public procurement system ProZorro, and other activities have greatly enhanced transparency and the fight against corruption. This unique hybrid public-private platform is internationally recognized for its out-of-the-box auditability and open-access design. The platform functions in compliance with the Law on Public Procurement and has received support from the USAID, EBRD, and the EU. The successful implementation of ProZorro alongside the Dozorro platform and Spending.gov.ua has shown that a combination of legal reform and digital change can achieve systemic transformation.

As previously emphasized, the effectiveness of these institutional changes is corresponding to the level of development of Ukraine's anti-corruption system. This includes the activities of institutions like the National Anti-Corruption Bureau of Ukraine (NABU), the Specialized Anti-Corruption Prosecutor's Office (SAPO), and the High Anti-Corruption Court (HACC). These institutions are backed by certain laws and also receive international technical and financial assistance. However, the autonomy of these institutions is still an issue, and the struggle to protect their autonomy and effectiveness is watched closely by the EU and Venice Commission.

One more notable component of financial integration is creation of internal capital market. Underdevelopment of capital markets in Ukraine leads to obstacles in raising investments and financial intermediation.

Reforms are being undertaken to bring Ukrainian legislation on securities into line with EU standards, particularly the MiFID II and Prospectus Regulation. The National Securities and Stock Market Commission (NSSMC) has started preparation for implementation of international financial reporting standards (IFRS) and enhancement of investor protection, but there is limited advancement on this front.

Public-private partnerships (PPPs) are also a new area of focus for Ukraine in the context of aligning itself with EU practices. The Law on Concessions (2019) and the updated PPP legislation serve as the legal framework for the attraction of private financing towards infrastructure development. Compliance with domestic laws and international financial obligations regarding investment is accompanied by the legal certainty, risk-sharing instruments, and transparent procurement frameworks.

The legal cooperation regarding financial supervision as part of the Ukrainian regime integrates the country into the European financial security framework. Ukraine has been working towards the alignment of its financial sector supervisory practices with the European System of Financial Supervision (ESFS) which encompasses the European Banking Authority (EBA), European Securities and Markets Authority (ESMA), and European Insurance and Occupational Pensions Authority (EIOPA). The Memoranda of Understanding between NBU and these international bodies create a channel for the exchange of supervisory information and the cross-border intelligence on capabilities and supervision systems.

To fortify credibility and governance, reforms within the oversight and auditing processes are fundamental. Accounting Chamber, Ukraine's Supreme Audit Body, is responsible for executing independent audits on the spending of state resources as well as international financial aid, scrutinizing even the international funds provided. The Chamber operates in accordance with the Law on the Accounting Chamber and tends to follow the international standards (ISSAIs) of supreme audit institutions. Technical support from international partners such as the EU and the World Bank is directed towards enhancing the effectiveness of the Chamber through training.

20.4. Strategic insights: from aid recipient to financial interactor in Europe

While implementing deep reforms toward institutional resilience and financial transparency, Ukraine needs to create a vision for itself as an

integrated and autonomous Europe's integrated and autonomous contributor and networked financial ecosystem. The shift from an aid-dependent country to a self-reliant actor in Europe's financial and security constellation requires meticulous foresight, legal evolution, and systemic change. This transition strategy is rooted in the concept of fiscal sovereignty. Ukraine becomes more independent with foreign assistance when the country is capable of mobilizing and managing domestic revenues, implementing stable tax regimes, and building fiscal forecasting abilities. Numerous advisory missions have suggested the broadening of the tax base through digital taxation, estate and wealth taxes, and better VAT compliance. These plans, however, need to be accompanied with a robust and investor-friendly legal environment, strong enforcement mechanisms, and impartial courts.

At the same time, Ukraine's financial legislation needs to keep pace with the latest market developments. Including reforms to the corporate governance code, the protection of minority shareholders, modernization of bankruptcy laws, and the creation of commercial arbitration systems. Legal certainty and the absence of conflict between the participants of the market and the state are necessary for the private and institutional investors to be able to.

The development of capital markets is one of the key elements of the further financial stability of Ukraine. There are prospects for diversification with the issuance of new instruments such as municipal bonds, green bonds, and sovereign bonds linked to economic growth. The law regulating these instruments must be aligned with the EU law on the Capital Requirements Directive (CRD V), the Securitisation Regulation, and the Sustainable Finance Disclosure Regulation (SFDR). The incorporation of environmental social governance (ESG) criteria into financial law of Ukraine will deepen alignment with the goals of the European Union.

Also, Ukraine needs to engage with regional financial efforts. This includes possible joining to the Single Euro Payments Area (SEPA), meeting the requirements of the Basel III and Basel IV frameworks, as well as joining the European Central Bank in its supervisory role over banking standards. Involvement in these structures will demand that Ukraine demonstrate alignment with the EU's financial *acquis* which is kept up-to-date and enforced through European Commission monitoring systems.

Besides structural and regulatory changes the broad aspects of culture and education also require attention geared towards the financial integration. Teaching and practice of European financial law for judges, regulators, and

civil servants requires some foresight to ensure success. Those engaging in pedagogy in the National School of Judges, the Ukrainian Academy of Banking, and law faculties in various parts of the country need to include EU financial legal frameworks in their syllabi.

Yet another dimension of change involves reframing with international financial institutions (IFIs) in relationships that are not based solely on borrowing. In regard to Eastern Partnership countries, Ukraine can become a donor or co-financing partner in a couple of years. These include engaging with regional World Bank projects or the EBRD's multi-country technical cooperation initiatives. Such collaboration would showcase Ukraine's growing institution maturity and offer them the opportunity to promote regional stability.

The domains of cybersecurity and financial technology are new areas of law requiring legislative development. With the growth of Ukrainian digital financial services, there is a need for legislation governing data protection, payment systems, fraud prevention, and blockchain technology. Ukraine can build a coherent and secure ecosystem of digital finance using the EU's Digital Finance Package and MiCA regulation as cornerstones. These laws also dovetail with wider security issues, particularly around safeguarding critical infrastructure from aggressive cyber operations.

On top of that, for further strategic shifts, Ukraine needs to facilitate self-governance along with public accountability. Monitoring public spending, their reforms, and advocating for policy change is the role of civil society, independent journalism, and academic institutions. Legal provisions enabling access to information, whistleblower protection, and civic oversight of budgetary processes require enhancement for effective monitoring.

Last but not least, upholding the rule of law is critical to consider for any strategy to transform Ukraine. A trusted judiciary, clearly defined property rights, adequate anti-corruption efforts, and a robust protection system for confidential and sensitive information continue to be mandatory for Ukraine's euromed integration. The annual EU Rule of Law Reports and recommendations from the Venice Commission provide milestones for deeper institutional convergence that Ukraine ought to fulfill consistently.

To sum it up, Ukraine's evolution from a post-conflict international-financial aid beneficiary to a European financial security partner is contingent upon an extensive legal, economic, institutional, and normative reform plan. Such transformation is not simply a reaction to a crisis but an active

strategizing concerning Ukraine's position in the regional and global stability ecosystem.

20.5. Ukraine's post conflict financial reconstruction legal frameworks

Ukraine's post-war reconstruction offers an unprecedented opportunity for establishing a governed financial management system that is aligned with European standards and adheres to the rule of law. While the conflict requires immediate and donor-sponsored fiscal emergency interventions, the post-conflict phase requires purposeful legal restructuring. Such restructuring should facilitate the reliable and equitable distribution of reconstruction resources, private investment acceptance, and the elimination of systemic weak spots.

A consolidated legal structure must look into several coordinated issues aiming at reconstruction. To begin with, a national planning and execution legal framework for reconstruction needs to be established. A legal document, such as a Reconstruction Law or Framework Act, will instate the guiding principles, institutional authority, and recovery oversight for post conflict reconstruction. It must have inbuilt transparency and public accountability, participation of the civil society, anti-corruption measures and ethnically cleansing criteria. Furthermore, it needs to outline the processes for donor coordination, budget rationalization, and international treaty obligations.

Also, the legal challenge of property restitution and compensation will be of utmost importance. Destruction of housing, businesses, and public infrastructure poses complex legal challenges concerning the restoration of ownership rights, evaluation of war damages, and compensation balance. Solutions pertaining to domestic legal mechanisms along with claim settlement adjudication processes such as special tribunals, administrative compensation schemes, international expertise hybrid mechanisms, will be required.

Thirdly, Ukraine's Parliament, as per constitutional procedures, needs to negotiate and ratify international legal agreements concerning reconstruction financing. These agreements need to abide by international standards and utilize models implemented in Europe after conflicts or other war-affected nations. There has best be provisions for accountability, resolution of disputes, and monitoring of progress. To There must also be legal safeguards to stress preventing debt distress and ensuring that

expenditures made through grants and loans are compliant with intended purposes.

Fourthly, legislation on infrastructure and procurement regulation will substantially contribute toward Ukraine's rebuilding efforts of its transport systems, energy systems, water management, and public buildings. The public procurement legal system must be shielded from elite capture or collusion, and also be aligned with EU benchmarks. Digital solutions such as ProZorro and blockchain contracting may provide these compractive barriers to manipulations. Nonetheless, there is need for reliable policy and strong judicial supervision alongside these.

As for the fifth point, a legal framework concerning sustainable development in reconstruction must ensure that there are legislative provisions on investment in green economy, energy efficiency, and urban resilient planning. Ukraine has developed climate legislation, and its incorporation into reconstruction planning can be enforced through regulatory mechanisms, licensing frameworks, and conditional financing contracts. Synergy with EU climate law, in particular the Green Deal and taxonomy regulation, would enable alignment of the reconstruction of Ukraine from an environmentally sustainable/European perspective.

For the sixth point, justice and anti-corruption policies need to be included in each and every level in relation to the legal framework of reconstruction. This applies to project selection, expenditure audit, criminal accountability for fund embezzlement, and safeguarding of whistleblowers. Independence for functional control is granted to Ukraine's NABU, HACC, and State Audit Office which legally empowers them to oversight these functions.

Last but not the least, legislative and constitutional reform is a moving target that must form part of the reconstruction process. Systemic governance gaps as a direct outcome of the war are evident in the areas of centralization, de-centralization, public administration, judicial sovereignty and public financing. An extensive framework of statehood doctrine puts forth the idea of formulating a cohesive national engagement in the approach to constitutional reforms that will proactively enshrine fiscal and institutional resilience as the bedrock of statehood. Instructing the legal experts, civil society alongside international partners would provide an inclusive approach to engaging with this design.

The path of Ukraine's recovery post-war is not only dependent on the amount of funding, but how the funds are structured legally. Ukraine needs

to receive funding in a way that ensures tangible growth to its territory, number of citizens, and more importantly the rule of law for it to be considered a European state. The system of law must also be developed as it will act as the framework for aid construction and provide protection over the evolution of Ukraine's democracy and economy.

20.6. Increasing Ukraine's participation in international financial institutions: goals and legal policies

Ukraine's strategy in international financing needs to shift from the periphery to prioritize regional focal points of international governance. Ukraine's engagement in frameworks concerning global financial regulations as well as international developmental assistance should be perceived as a hallmark of statehood, patriotism, and sovereignty and in fact a hallmark to Ukraine's power and durability.

Legal and policy pathways are suggested in this chapter to facilitate Ukraine's advancement from an IFO (International Financial Organization) recipient status to contributor within IMF, World Bank, EBRD, FSB and IOSCO. These institutions are the pillars of international governance setting benchmarks for monetary policy, banking and debt management, and capital mobility – all of which will be crucial for determining the future economic growth of Ukraine's economy.

As we have argued before, Ukraine's advanced participation in global finance requires upgrading its legal representation in international relations. Expanding voting to the extent possible, providing greater participation in technical committees, attending peer review sessions, and drawing up reform agendas aligned with the needs of emerging economies affected by war and transition are steps in the right directions. It will also be necessary to change laws concerned with Ukraine's representation at international organizations and the appointment processes to ensure strategic attendance and capability.

Moreover, Ukraine can serve as an exemplary post-conflict advocate for financial justice and international law reform. Ukraine's history of war provides a rationale for Ukraine leading global initiatives developing legal frameworks for economic injury inflicted by war, asset seizure, and legal reparations. Ukraine could sponsor a law on reconstruction finance governance or set international standards on equitable debt restructuring and donor transparency.

Third, Ukraine should focus on forging agreements with global apex institutions to expand cooperation with the Basel Committee on Banking Supervision, the International Accounting Standards Board (IASB), and the OECD through formal memoranda and joint technical initiatives. Investment into aligning Ukraine's banking and corporate regulations with global standards will enhance the credibility of its financial system, attract foreign investments, and reduce regulatory barriers for international trade.

Fourth, Ukraine needs to resolve the legal and functional issues pertaining to participating in, and exercising influence over, regional development programs such as the EU's InvestEU program, the Three Seas Initiative Investment Fund, and the Black Sea Economic Cooperation financial frameworks. Harmonization of the law, sovereign guarantees, and co-financing will make these funds easier for Ukraine to access, thus enhancing competitiveness.

Fifth, the nation ought to set up a National Platform for International Financial Cooperation, which would include a representative from the Ministry of Finance, National Bank of Ukraine, Parliament, as well as civil society and scholars. This platform would help to unify Ukraine's international representation and ensure policy-making in foreign finances is transparent and accountable. Enabling legislation could form this body as an independent agency placed under the Parliament's supervision.

Sixth, there is an absolute need for a legal approach geared towards diplomacy for sustainable financing. Domestic reforms need to be made in law of sustainability disclosure, climate finance, and socially responsible investment to adequately support Ukraine's participation in ESG (environmental, social, governance) frameworks. Ukraine's leadership role in sustainable post-conflict recovery finance will be strengthened through engagement with the Task Force on Climate-related Financial Disclosures (TCFD) and adopting the EU Green Bond Standard.

Ukraine needs to proactively engage in international legal processes; for this, Ukraine has to focus on developing its resources for international financial law and diplomacy. Setting up specialized university departments, scholarships with international placements, and public service pathways in financial diplomacy will nurture long-term expertise. Such investment in human capital enables Ukraine to actively shape global policies rather than just comply with them.

To wrap it up, the Ukraine case study added to this study pointed out that there should be incorporation of advanced legal frameworks that allow

for a preventive approach towards sustaining financial crises. On the global and European level, Ukraine gaining access to international finances hinges on applying proactive legal measures alongside building strong institutions that foster diplomacy. That proactive anticipation towards law making will determine if Ukraine can be a driving force in aiding the construction of a more equitable, robust and rule-abiding international financial framework that proactively contains, mitigates, and recovers from global turmoil.

The array of fiscal and institutional obstacles posed toward Ukraine as a blunt force challenge due to the full Russian invasion opened up opportunities for configuring laws aimed to sustain lesser shocks in capitalism's cyclic nature. Relying purely on emergency measures and international aid will ensure a lack of stability focused over sustainability, especially when considering how the reconstructing Ukraine economy is reliant on the development of durable legal designs systems that are meant for fundamental, structural shocks.

Structural shocks require re-evaluating whole system designs which enable jurisdictions to endure crises directed at systems and simultaneously strengthen their efficiency toward external changes. In this regard Ukraine has to be approached from numerous angles for vertical and horizontal integration, not limited to but including fiscal and budget statutes, banking and financial control, anti-corruption, emergency legislative powers, and institutional framework design.

First, Ukraine illustrates the necessity of having defined constitutional frameworks involving finance governance in relation to emergencies. Put into action, the absence of defined rules pertaining to the monetization of the deficit, the autonomy of the central bank in wartime, and borrowing in times of emergency all work against promoting swift decision-making. These issues require amendments to the constitution and statutes clearly defining the bounds of constraining power defined as a financial state of emergency in order to maintain democratic control over processes while retaining the required agile execution.

In the second place, flexibility in fiscal law needs to be considered alongside its strong procedural guarding safeguards. The state budget system should include some emergency reallocating provisions, expenditure planning, fiscal risk assessment, and other forms of public and parliamentary scrutiny. Stricter oversight by the Ukrainian Parliament in the budget process, alongside increased emergency spending, requires greater public attention and oversight. While Ukraine's changes to the Budget Code in 2022 and 2023

were steps forward, further protocols should rigidly outline substantive jump-over loopholes regarding fiscal emergencies.

In the third place, the legal framework should guarantee the uninterrupted existence and functioning of independent bodies throughout the entire period of emergency. Operational and legal independence of the National Bank of Ukraine (NBU), Accounting Chamber, and the Anti-Corruption institutions is critical for the trust of investors and institutional credibility. These entities need protection against political and legal reform changes that would allow for remote governance and digital crisis mode resilience across the entire set of decision-making processes.

Finally, changes in procurement law, public-private partnerships, or PPPs should allow for ordered expansion and unrestricted accessibility in times of crisis. While Ukraine's ProZorro system is a notable success, additional legislative measures are necessary in order to guarantee expedited yet responsible public procurement in emergencies, especially defining force majeure, framework agreements, and audit triggers.

Fifth, in a proactive approach to the law, scenario planning and planning for legal stress tests *ex ante* should be incorporated. Governments alongside other stakeholders could establish frameworks towards the development of legal stress tests that analyze the enduring nature of financial laws and regulations within timeframe-crisis simulations. This would require the cooperation of legal experts, economists, and policy makers.

Sixth, public trust is best achieved through legal design work that is centered around the citizens which is an experience that Ukraine shows us. In times of crises, open legal communication, accessibility to public spending information, and mechanisms for participatory budgeting enhances democracy even under stress. Legal protection of such information must be provided and digital rights guaranteed, and these must be honored even during times of emergency.

Seventh, the order through which international aid and the resultant scrutiny from donors is channeled needs to be streamlined within the Ukraine legal system. Establishing a legal policy on the oversight of external assistance to cover project selection, auditing, sanctions for misuse, and civil society participation will effectively channel international assistance into developmental results. This is important to note because as the reconstruction takes place at a heightened pace, there is a risk of donor fatigue.

At long last, Ukraine needs to integrate its legal frameworks to ensure resilience within a National Law on Economic Security and Crisis

Preparedness, which would define the principles, institutions, and processes required for governance that is effective and resilient. This law could act as a guide for other states grappling with conflicts or in transitional phases, striving to establish control over finances amidst volatile geopolitical situations.

To sum up, the case of Ukraine showcases the attempt to strengthen finances from a legal governance approach during wartime and how it poses important lessons for dealing with other disruptive scenarios. Incorporating these findings into enforceable legal policies will be imperative to achieve sustainable resilience, not only for Ukraine, but also for the entire European and global financial system.

In synthesis, Ukraine's case illustrates that in recovery, money is not the primary issue. Instead, it is law, legitimacy, and institutional order. As we already indicated, cross-border bodies need to fulfill their role as both providers and guardians in this recovery and active flow of finances needs to be complemented with normative elaboration. At the same time, Ukraine needs to strengthen the legal and institutional framework in order to become actively benchmarked in the European and global community of finance.

Therefore, the Ukrainian path to financial resilience is both a test of national endurance and contributes to the emerging 21st century security architecture where law, finance, and sovereignty blend seamlessly.

References

1. European Commission. (2023). *EU Support to Ukraine*. Available at: <https://ec.europa.eu>
2. International Monetary Fund. (2023). *Ukraine Extended Fund Facility Arrangement*. Available at: <https://www.imf.org>
3. World Bank. (2023). *Ukraine: Country Overview*. Available at: <https://www.worldbank.org>
4. European Bank for Reconstruction and Development. (2023). *EBRD's Response to the War in Ukraine*. Available at: <https://www.ebrd.com>
5. Multi-agency Donor Coordination Platform. (2024). *Progress Report*. Available at: <https://www.platformukraine.org>
6. Ministry of Finance of Ukraine. (2024). *Public Reports on External Assistance*. Kyiv: Ministry of Finance.

7. OECD. (2022). *Ukraine Recovery and Reconstruction Needs*. Paris: OECD Publishing.
8. National Bank of Ukraine. (2024). *Financial Stability Report*. Kyiv: NBU.
9. Transparency International. (2023). *Corruption Perceptions Index: Ukraine*. Available at: <https://www.transparency.org>
10. KPMG Ukraine. (2023). *Reforming Ukraine's Financial Sector: Challenges and Opportunities*. Kyiv: KPMG.
11. European Court of Auditors. (2023). *EU Financial Assistance for Ukraine – Special Report*. Luxembourg: ECA.
12. Ministry of Digital Transformation of Ukraine. (2024). *Diia Platform Annual Report*. Kyiv.
13. USAID. (2023). *Building Resilience through Digital Financial Management Systems: Ukraine Case Study*. Washington, D.C.: USAID.
14. World Economic Forum. (2023). *Global Competitiveness Report – Ukraine Profile*. Geneva: WEF.
15. International Monetary Fund. (2022). *Lessons from Post-Conflict Economic Reconstruction: Selected Case Studies*. Washington, D.C.: IMF.
16. Basel Committee on Banking Supervision. (2023). *Basel III: Finalising Post-Crisis Reforms*. Basel: Bank for International Settlements.
17. European Central Bank. (2023). *ECB Convergence Report 2023*. Frankfurt am Main: ECB.
18. European Commission. (2024). *Green Deal and Ukraine's Integration Path*. Brussels: EC.
19. Venice Commission. (2023). *Opinion on the Independence of Anti-Corruption Institutions in Ukraine*. Strasbourg: Council of Europe.
20. International Organization of Securities Commissions. (2023). *Annual Report*. Madrid: IOSCO.

Chapter 21

Investment case of post-war recovery of Ukraine: cross-border hydrogen clusters, near-shoring, innovation taxation (O. Borodina)

The long-term resistance to Russian aggression has put Ukraine's economy in a war mode with a large number of restrictions that are significantly felt and will have a significant negative impact on the further development of the state. It is quite obvious that the post-war recovery of the Ukrainian economy must and will take place with the support of international financial institutions and funds – both public and private. It is appropriate to state that the world community is currently demonstrating its readiness to consolidate assistance to the affected Ukrainian economy by creating joint mechanisms for infrastructure reconstruction, institutional modernization and economic transformation.

In turn, the Government of Ukraine presents strategic documents for the post-war recovery and development of Ukraine [1] at various international platforms, focused on creative mechanisms for economic recovery as a guarantee of sustainable development.

The arsenal of examples of effective cases of post-war development of national economies is quite significant. However, for the most part, analytical reports only mention the Marshall Plan as a program for the reconstruction of post-war Western Europe [2].

At the same time, noting the undeniable success of the Marshall Plan in achieving its goals, we note that the complexity and uniqueness of the conditions in which Ukraine will find itself after the end of hostilities determines the need for a comprehensive approach to finding a model of post-war economic development. Moreover, we are not talking about the direct reconstruction of the destroyed infrastructure, but about

the possible radical transformation of the state into a modern, modernized and comfortable smart environment for life. Given the extremely heavy price that Ukraine is forced to bear, we must use this opportunity as effectively as possible. At the same time, the context of historical comparisons includes examples of no less successful cases of rebuilding the destroyed national economy and further rapid economic development [3].

The problems of strategizing the crisis economy, including cluster instruments for ensuring regional policy, are actively considered by foreign economists. Thus, in modern conditions of decentralization, the use of a structured regional approach is considered one of the most effective mechanisms for structural development of the economy [4].

At the same time, the unprecedented conditions of today in Ukraine, namely - colossal losses as a result of military actions, which only continue to increase; specific and unique geopolitical, economic, social conditions in which the country found itself in this military confrontation; the important place of Ukraine in the world market of food, energy, metallurgy, determine the extreme importance of using the most effective creative tools and methods of post-war economic recovery. These, in our opinion, are, for example, the development of hydrogen energy, the introduction of the near-shoring mechanism, as well as the implementation of the European experience of innovative taxation (the experience of the tax on withdrawn capital).

21.1 Cross-border hydrogen clusters

Climate neutrality and ‘green’ transition – modern trends in the development of the European Union [5] In the coming years, the development of the energy sector, in particular, the production of ‘green’ energy for domestic needs and exports to the EU, will become one of the priority areas of development of the Ukrainian economy.

Ukraine has supported the EU's ambitious plan to achieve climate neutrality. The situation is also made more urgent by the fact that, as part of post-war reconstruction, Ukraine will have to rebuild some industries practically from scratch. It is important that this reconstruction be a qualitative transformation, innovative modernization. There is an urgent need to explore potential opportunities in the country's regions in order to offer them as investment beacons, undoubtedly taking into account the trends of modern development and the focus of attention of future donor countries.

It is extremely important to use European, primarily Polish, experience to implement new trends in the hydrogen economy in Ukraine. Thus, Poland is actively preparing the potential for a leading role in the European "hydrogen" revolution, in particular, it is mobilizing the efforts of the private and public sectors of the economy in order to take a competitive position on the "hydrogen" map of Europe, which in turn opens up significant investment potential for the post-war development of the Ukrainian economy [6].

The key recent theses in this direction in the EU are as follows:

1. The current acceleration of the European hydrogen market is relevant. At the EU level, there is a transition from the planning phase and theoretical discussions to the phase of real activity at each stage of the value chain.

2. The Russian invasion of Ukraine and the resulting energy crisis are accelerating the decarbonization of the European economy, including the use of green hydrogen. While crisis management tools may increase the importance of fossil fuels in the short term, renewable energy will become more important in the medium and long term. At the same time, the sharp increase in the price of natural gas is leading to a several-fold increase in the cost of producing grey hydrogen, which strengthens the price competitiveness of 'green' hydrogen.

3. By 2030, the main focus will be on decarbonizing certain sectors of the economy: oil refining, chemicals, steel. This does not mean marginalizing other possible applications in the fields of transport, energy or heating, but the hydrogen industry has every reason to become a driving force of the hydrogen economy both in Europe and in other parts of the world.

4. Poland is currently in the middle of the list of member states with ambitions for the development of the hydrogen market, it has a good starting position, which is the result of the fact that the country is a leading producer and consumer of grey hydrogen. At the national level, a regulatory framework for the development of the green hydrogen market has been prepared. A

social consensus has developed around the issue of clean hydrogen – a wide range of stakeholders are involved in the work of various types of clusters, valleys and associations, who see and appreciate its potential.

5. Poland will maximally activate institutional and legislative work in the coming years and plans to play a key role in the water map of Europe [7].

The attractiveness of green hydrogen is primarily explained by its potential for use in those areas of life where decarbonization is the biggest problem and cannot be achieved solely on the basis of electricity from renewable energy sources, which by its nature is characterized by a lack of controllability.

The potential for green hydrogen goes beyond replacing grey hydrogen. It encompasses a wide range of possible applications in industries that have not historically used hydrogen or have only used it at the pilot level (Fig. 21.1).

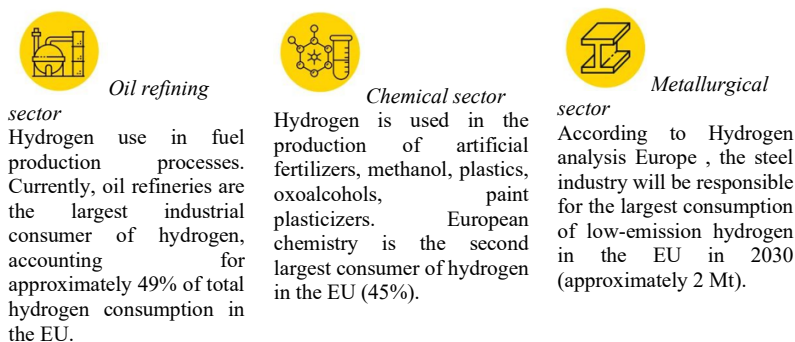


Fig. 21.1. Priority use of 'green' hydrogen in the process of decarbonization of EU industry

Compiled by the author based on [8]

The potential volume of 'green' hydrogen production in Ukraine was calculated by the Institute of Renewable Energy Sources of the National Academy of Sciences of Ukraine (IRE) based on the results of scientific research into the potential for electricity generation by wind and photovoltaic stations. To calculate the potential volume of "green" hydrogen production by electrolysis, specific consumption is assumed electricity 4.5 kWh /n m³ N₂ or 50.56 kWh /kg H₂ [9].

According to data calculated by the Energy and Power Engineering Institute of Ukraine (Table 21.1), the estimated forecast for the production of 'green' electricity and hydrogen exceeds the calculations of the Energy Strategy of Ukraine approved before the war for the period until 2035.

Table 21.1

Estimated forecast for the production of 'green' energy and hydrogen*

year		2025	2030	2035
Energy strategy	billion kWh	12	18	25
	H ₂ (billion nm ³)	0.6	0.9	1.2
IBE calculations	billion kWh	21.6	35.5	52.5
	H ₂ (billion nm ³)	1.1	1.8	2.6

**Source: compiled by author based on: [8,9]*

Thus, the production potential in Ukraine will be sufficient for both domestic needs and export. At the same time, the optimal territories for hydrogen production, according to calculations by specialists of the Institute of Energy and Environmental Sciences of the National Academy of Sciences, are the following regions of Ukraine:

- the highest possibility, at the level of 24,700 million nm³/year – Dnipropetrovsk region;
- volume 22173 million nm³/year – Odesa region;
- volume 22021 million nm³/year – Kherson region.

The prospect of Zaporizhia and Donetsk regions is very attractive (with the last three regions mainly due to wind energy in electrolysis).

Thus, the cluster prospects of the old industrial regions of Ukraine in introducing such production are unconditional. And taking into account the offshore potential and technologies of possible water desalination, Donetsk, Zaporizhia, Kherson regions can become the main hydrogen hubs of the country. In general, Ukraine can produce more than 500 billion cubic meters of green hydrogen per year. This will be enough for both domestic needs and export.

The advantages of hydrogen do not end in production. It can also be used as a means of storing excess electricity from renewable sources, when its production exceeds demand – then it becomes a kind of battery. That is, hydrogen can solve two problems at once – harmful emissions and the difficulty of "conserving" energy from renewable sources.

In addition, compressed hydrogen gas, according to recent research, can be stored profitably in underground salt caves. According to Hydrogen Europe Industry Board, storing hydrogen energy in salt chambers is at least a hundred times cheaper than storing electricity in energy storage [10] .

According to the industry's technological regulations, hydrogen storage is a key component in hydrogen supply. Choosing the most suitable storage technology is a balanced decision between the amount of hydrogen, its storage (e.g., tank size) and energy use.

Hydrogen storage potential in Ukraine.

Hydrogen can be stored in liquid and compressed gaseous states not only in tanks or cylinders/containers, but also underground in salt caves, depleted oil and gas fields or aquifers, as well as in sections of gas pipelines that have already been decommissioned. Existing salt chambers left after the depletion of salt mines are the most promising option for hydrogen storage, given the European Union's ambitious plans to integrate hydrogen technologies into various industrial sectors, with the aim of decarbonizing the latter.

Storing hydrogen energy in salt chambers is more cost-effective than storing electricity in an energy storage facility. In addition to salt chambers, great potential has been demonstrated for new storage tanks in salt layers. In addition, hydrogen can probably be stored in some depleted gas fields. And here, as best we can offer Western investors the potential of salt mines and caves, as well as on decommissioned or operating sections of gas pipelines in old industrial regions of Ukraine (when the gas pipeline itself becomes a reservoir).

Zaporizhia, Donetsk, Dnipropetrovsk regions, cities in Transcarpathia have industrial infrastructure facilities that were actively used as mines, including salt mines, before the start of hostilities, and therefore, if investments are available, they can be restored in post-war development for use in the hydrogen infrastructure cycle.

Cost of storage. Hydrogen storage is a key component in securing the resource. Choosing the most appropriate storage technology is a trade-off between the amount of hydrogen, its storage (e.g., tank size), and energy use. Compressing gaseous hydrogen is the most attractive option for long-term storage, given its relatively low cost and greater availability. Combined with possible improvements in compression efficiency, hydrogen storage is expected to add \$0.3 per kg to the cost of hydrogen production by 2025. At the same time, the cost of the technology is expected to decrease

Ukraine's potential in hydrogen transportation.

Hydrogen transportation via pipelines also has an advantage over electricity transmission, as hydrogen can be relatively easily stored and stored in underground and above-ground pressurized storage facilities and delivered via pipelines to consumers on demand at a predetermined time and in controlled quantities. In this regard, the construction of hydrogen pipelines is promising. Protecting such transport routes from hostile environments requires significant investment, but a ready-made hydrogen pipeline is the cheapest way to deliver large volumes of hydrogen. The development of a network of specialized pipelines could also make hydrogen the cheapest way to transmit electricity over long distances.

The use of the gas transportation system of Ukraine enables its efficient transportation. (Table 21.2).

Table 21.2

General technical characteristics of the GTS of Ukraine*

Technical characteristics	Unit of measurement
Length gas pipelines	38.9 thousand km
Length main roads pipelines	22.2 thousand km
Pass input capacity	288 billion cubic meters per year
Pass output capacity	178.5 billion cubic meters per year
Pass EU exit capability	146 billion cubic meters per year
Number gas transportation units	702 pcs
Number compressor stations	72 pcs
Electric power compressor stations	5448.0 MW

Source: compiled by author based on [8,9]

In this case, it is quite likely and relevant to develop a full-cycle hydrogen project for implementation in the energy sector of Ukraine – from the production of hydrogen and its derivatives (for example, ammonia), to its transportation and storage.

So, hydrogen is exactly the resource that can make money for Ukraine. It is the energy sector of the Ukrainian economy that can become a platform

for implementing the concept of *nearshoring* (outsourcing to a country relatively close to the main country of business). That is, it can make the Ukrainian energy sector a mega-industrial park for Europe. The advantages for both sides are obvious. For Ukraine, it is an influx of investments that are extremely necessary for the restoration of the economy, the revival of the destroyed infrastructure of old industrial regions, which will certainly become drivers of the post-war regional development of the national economy. For the EU, it is the availability and possibility of using full-cycle infrastructure to ensure a ‘green’ decarbonized transition and, in the future, achieving the level of a climate-neutral continent.

In our opinion, the following measures are considered necessary to create a national climate governance architecture in Ukraine:

- development and adoption of a full-fledged and extensive modern industry regulatory framework (laws, subordinate regulations, strategic documents),

- implementation of EU rules at the national level in order to prevent excessive market centralization, creation of a network of "Hydrogen Valleys" based on the old industrial regions of the state,

- combination in regulatory documents of two systems of planning for the development of the green hydrogen market: ‘Top-down’ (the central role of the state and its planning bodies) and ‘bottom-up’ (the activities of local governments and local initiative),

- preparation of a green hydrogen roadmap in national industry, activation of conceptual work in the field of hydrogen logistics

- training of highly qualified personnel who have an understanding of hydrogen technologies and their use.

- development of R&D. Involvement of Ukraine’s scientific potential in studying hydrogen technologies, reducing the cost and improving the quality of hydrogen, and studying new areas for hydrogen application.

- creating consumer demand through consumer awareness of the benefits of hydrogen, hydrogen technologies and fuel cells, popularizing cases of successful use of hydrogen in the automotive industry, power generation, and industry.

Of course, hydrogen energy is an innovation and it is not worth talking about it as a real preferential prospect in the next 5–10 years, and the topic of hydrogen around the world is still far from mass production. However, the mutual interest of investors external to Ukraine, which, moreover, is based on European program documents, puts the hydrogen prospects of the energy

sector of Ukraine in the category of investment beacons to ensure effective post-war recovery.

21.2. Nearshoring

In the context of post-war reconstruction and political turbulence, when under natural circumstances the value of state assets decreases, we consider it a reasonable state decision to apply international assistance programs based on the principles below (Table 21.3), to concentrate efforts on increasing the efficiency of the public sector of the economy, to accumulate funds and carry out industrial modernization, and to invest in innovation and science.

The key task is to provide investors with mechanisms to maximize development: compensatory mechanisms for losses, or connection to engineering networks. Priorities for the development of the processing industry, the development of industrial parks. A promising concept of nearshoring is the transformation of Ukraine into the nearest industrial zone (mega-industrial park for Europe). And this, in turn, will actively stimulate the development of the services sector [11].

The terms of using this format of relations are mutually beneficial both for Ukraine (with the attraction of foreign investments and rapid renewal of industrial capacities) and for Western partners (since the governments of European countries can provide state guarantees to companies investing in Ukraine). The innovative business model of nearshoring has been adopted worldwide in the private and public sectors due to its numerous advantages.

For European partners, *the advantages of Ukraine in the context of nearshoring* in the energy sector are as follows:

1. Ukraine is a highly educated country, with a sufficient pool of qualified technical specialists. The quality of Ukrainian higher education is recognized worldwide. A fairly large percentage of specialized specialists are engineers.

2. A reasonable combination of price and quality. The price of domestic electricity is absolutely acceptable for the European consumer, at the same time, synchronization with the European energy system has made it possible to ensure European standards, including quality standards.

3. Synchronization of accounting due to the proximity of time zones of Ukraine and the EU. Given the practically minimal gaps in time zones between Ukraine and Europe, such a business model will satisfy both the producer and the consumer. Ukraine, being in the center of Europe,

conveniently crosses time zones with European countries with minimal deviations.

Table 21.3

Principles for implementing international assistance programs that will be effective for the post-war economy of Ukraine*

Principle	Essence
<i>Sources of assistance</i>	Comprehensive multilateral international assistance from partner countries, led by the USA, EU, and UK
<i>Conditions of assistance</i>	– real work of anti-oligarchic laws, – fighting corruption, – reform of the law enforcement sector
<i>Development approach</i>	Focusing attention on the tasks of creating opportunities in all areas of economic and social development, radical transformation for rapid and high-quality new development
<i>Jointly Coordinated Efforts</i>	Coordination of joint actions of the National Council for the Recovery of Ukraine from the Consequences of the War and the relevant international structures established on an advisory and consultative basis
<i>Multi-stakeholders' implementation</i>	Involvement of international experts, Ukrainian scientists, financial and business circles, representatives of security and legal structures
<i>Modernization Perspective & Mutual Benefit</i>	Transforming Ukraine into a modern country with a qualitatively updated industrial infrastructure, innovative potential, investment attractiveness, a mega-industrial park and a logistics hub for Europe
<i>Risks for Ukraine</i>	Ensuring anti-corruption measures, real control over the targeted use of resources and funds, transparency of public procurement, accountability and tax discipline

Source: compiled by the author based on [3,7]

The key basic condition for effective development is the achievement of predominant localization in the use of own resources. At the same time, Ukraine is also interested in introducing the concept of nearshoring into the country's economic field, and not only in the energy sector. The possibility of using the logistics, industrial, and intellectual potential of Ukraine to create the nearest industrial site with active development of the service sector, primarily IT technologies, logistics, and innovations, is becoming promising.

Ukraine's access to EU markets, which cover more than half of the world economy, will also be an absolute advantage. This is not only export,

but also technology transfer to Ukraine, which is no less important for industrial modernization.

Currently, Europe's energy balance is dominated by high dependence on a single supplier, which negatively affects the Commonwealth economy, reducing the competitiveness of its industry and other related business sectors at the global level.

21.3. Innovative taxation (tax on withdrawn capital)

Another argument for correlating and taking into account the experience of Poland is fiscal innovations and special tax regimes. Thus, the introduction of a capital withdrawal tax (Estonian CIT, because it was Estonia that first introduced this innovative tool into its own taxation system) and even its modernization for the needs of small businesses from 01.01.2023, demonstrate a positive effect [12]. At the same time, Ukraine, which several years ago began discussing the introduction of a capital withdrawal tax, largely under pressure from the IMF, due to the indecision of politicians and the lack of guaranteed compensatory mechanisms for replenishing budget losses, has not been able to advance its introduction further beyond political promises and the introduction of bills to parliament without the aim of implementation. Time and opportunities have been lost, and our neighbor Poland is confidently moving forward.

The capital outflow tax is a mechanism for diversifying the development of regions, including those with a large number of relocated enterprises [13]. The stimulating role of such a preferential taxation regime for the post-crisis economy of Ukraine is obvious: incentives are created for business and investment activity, the projected 'loss regime' can last about 2–3 years, favorable conditions are created for determining the financial result of an enterprise, which does not need to underestimate the financial result for taxation purposes, simplification of fiscal control will contribute to the revival and development of the business environment; simplification of doing business will be a positive signal for foreign investors and GDP growth. Based on this, we can state the main advantages of the Estonian SIT for Ukraine: de-offshorization; stimulation of business entities to leave profits for expansion and renewal of production; avoidance of aggressive tax planning schemes, when the enterprise is deliberately made unprofitable in order not to pay income tax; reducing the corruption component due to

greater simplicity and transparency of the administration of the new tax, and as a result, attracting investment [14].

It should be noted that Poland and Estonia have radically different tax systems. While consumption and property tax policies are the main deterrents, Poland can also benefit from corporate tax reforms. Poland has adopted the Estonian approach to business taxation and has decided to implement a similar reform. The Polish government has adopted new tax rules for small businesses from the beginning of 2021 [15].

In order to increase the efficiency of tax law enforcement, the Polish government carried out an ‘overhaul’ of the Estonian CIT in 2023, which had the following consequences:

- the tax became available not only to small businesses, but also to all companies, regardless of their annual income;
- obligations to incur investment costs for certain purposes in a certain amount are completely canceled;
- limited liability companies and joint-stock companies have been added to the list of legal forms of companies that have access to the tax.

The variant of the advantages of the Estonian SIT 2.0 is shown in Fig. 21.2.

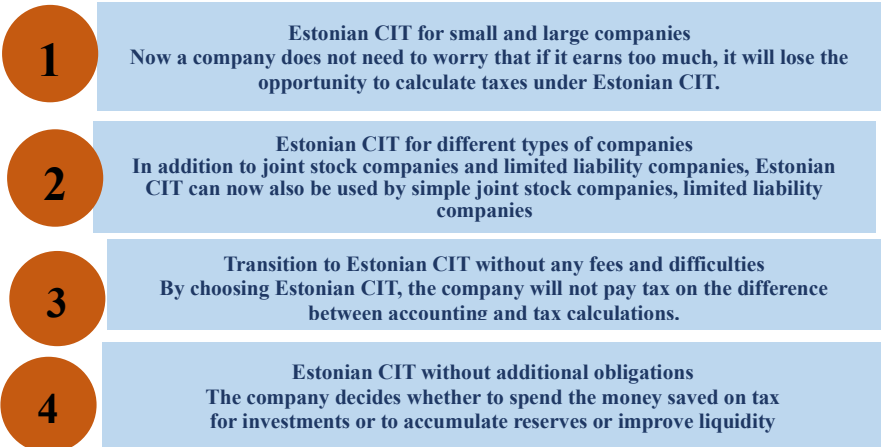


Fig. 21.2. Advantages of the Estonian CIT version 2.0, which came into force on January 1, 2023

Compiled by the author based on [8,9]

The stress resistance of the taxation system for foreign investment in some European countries and the EU as a whole, which is extremely important for the post-war economy of Ukraine, is demonstrated by Fig. 21.3.

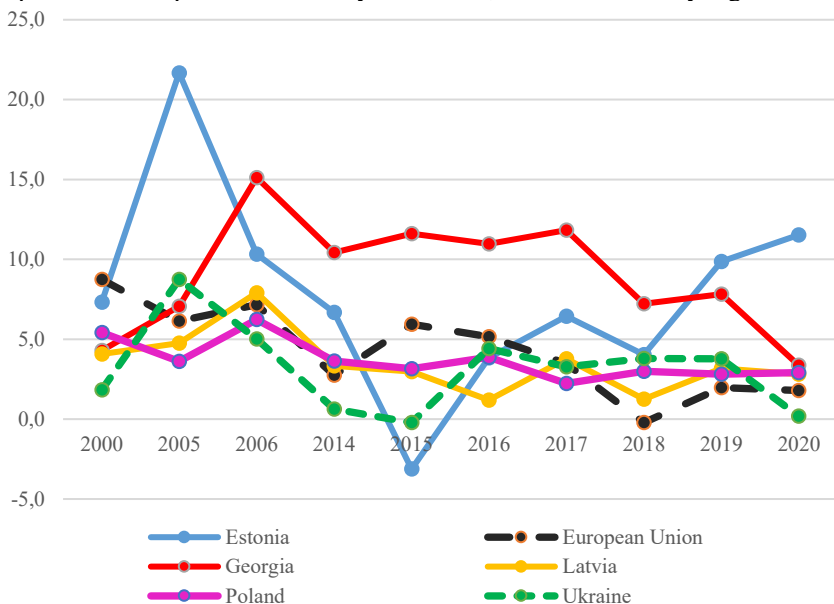


Fig.21.3. The volume of foreign direct investment inflows, as a percentage of GDP, in some European countries

Compiled by the author based on [16]

As we can see from the diagram, the Estonian tax system, even in the conditions of the crisis caused by the 2019 pandemic, demonstrated an increase in the volume of FDI, confirming its first place in the ranking of competitive tax systems in the world.

Poland and Latvia have also had stable positions over the past few years. Ukraine, on the other hand, had negative FDI growth during the COVID-depression.

A number of factors oppose the introduction of a tax on withdrawn capital in Ukraine:

- opposition from companies that are no longer going to invest in development in Ukraine, and they have a decisive influence on the IMF's position;

– insufficient determination of governments, which may face a difficult task – to go through the transition period, applying maximum intelligence and skill in managing systemic reform;

– unwillingness/inability of the authorities to defend the interests of Ukrainian business.

In turn, the IMF expressed serious concern about the loss of state budget revenues, which could be critical for Ukraine, so in the memorandum on economic and financial policy that Ukraine concluded with the International Monetary Fund after the last review of the credit program, the authorities pledged not to replace the income tax with a tax on withdrawn capital. There is reason to assume that the tax on withdrawn capital will bring less income tax to the budget in the first two years, but in the third year, revenues will increase sharply, covering the shortfall of the first years, while giving about 7% of GDP instead of the current 2–3%.

Summarizing the above, it can be noted that:

1. If the country's economy is not restored after the war, it will need to be constantly subsidized. And the latter ends up being much more expensive.

2. The phased recovery of the economy of post-war Ukraine, regional and sectoral development should be built on the basis of synergistic effects in conditions of limited resources and large-scale losses, depending on the scale of destruction and the availability of funds.

3. The Ukrainian economy has significant potential for activating industrial development, in particular through the mechanism of industrial parks under the conditions of implementing a package of reforms aimed at increasing the investment attractiveness of industrial parks.

4. Within the framework of Ukraine's post-war recovery, it is urgently necessary to implement an industrial reform package aimed at bringing the attractiveness of economic activity conditions in Ukraine's industrial parks closer to the level of neighboring countries (Poland, the Baltic countries, Turkey, etc.), which will include incentives for reinvesting profits in industry and science, exemption from land tax for industrial lands, free connection to engineering networks (at the expense of the investment component of tariffs), giving preference to Ukrainian products in public procurement, and implementing large-scale infrastructure projects on the basis of public-private partnership.

5. There is no doubt about the need for a comprehensive solution. The problems are not only changing the taxation system, but also implementing a whole range of legislative changes in the field of business and investment

protection, protection of private property and ensuring other guarantees, rights and freedoms. The main advantages of the Estonian SIT for Ukraine (even if its existence is temporary) are the following:

- deoffshorization;
- encouraging business entities to leave profits for the expansion and renewal of production;
- avoiding aggressive tax planning schemes, when a company is deliberately made unprofitable in order to avoid paying income tax;
- reduction of the corruption component due to greater simplicity and transparency of the administration of the new tax. As a result, attracting investments.

The classical model of corporate income taxation in Ukraine is ineffective. In the conditions of post-war restructuring, not only quantitative but also qualitative transformations are appropriate, a fundamental change in the philosophy of management, and innovative modernization, which, in our opinion, will become the driver of the post-crisis economic development of the state.

References

1. Ukraine recovery plan (2022). Available at: <https://recovery.gov.ua/>
2. Marshall, A. (1890). Principles of Economics. Available at: <https://eet.pixel-online.org/files/etranslation/original/Marshall,%20Principles%20of%20Economics.pdf>
3. Borodina, O. A., Lyashenko, V. I. (2022). Post-war economic recovery: world experience and an attempt to adapt it for Ukraine. *Bulletin of Economic Science of Ukraine*. No. 1 (42). P. 121–134. [https://doi.org/10.37405/1729-7206.2022.1\(42\).121-134](https://doi.org/10.37405/1729-7206.2022.1(42).121-134).
4. Pyatinkin, S. F., & Bykova, T. P. (2008). Razvitie klasterov: sushhnost', aktual'nye podhody, zarubezhnyj opyt [Development of clusters: essence, actual approaches, foreign experience]. Minsk: Tesej.
5. European Commission. A European Green Deal , 2019. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en
6. "Перехід України на відновлювану енергетику до 2050 року" / О. Дячук, М. Чепелев, Р. Подолець, Г. Трипольська та ін.; за заг. ред. Ю. Огаренко та О. Алієвої. Пред-во Фонду ім. Г. Бюлля в Україні. Київ: Вид-во ТОВ "АРТ КНИГА", 2017. 88 с. Available at:

https://ua.boell.org/sites/default/files/perehid_ukraini_na_vidnovlyuvanu_e_nergetiku_do_2050_roku.pdf

7. Lyashenko, V. I., Borodina, O. A. (2024). Energy decentralization as a path to energy security: the experience of Poland for Ukrainian communities. *Bulletin of Economic Science of Ukraine*. No. 2 (47). P. 22–34. [https://doi.org/10.37405/1729-7206.2024.2\(47\).22-34](https://doi.org/10.37405/1729-7206.2024.2(47).22-34)

8. Atlas of the energy potential of renewable energy sources of Ukraine / edited by S. O. Kudri. Kyiv: Institute of Renewable Energy of the NAS of Ukraine, 2020. 82 p.

9. Hydrogen Strategy of Ukraine: Project. Institute of Renewable Energy of the National Academy of Sciences of Ukraine. Kyiv, 2021. 91 p. ISBN 978-966-999-220-8

10. Global Hydrogen Review 2023. Available at: <https://www.iea.org/reports/global-hydrogen-review-2023>

11. Borodina, O., Bratus, H., Udovychenko, V., Kaczmarzewski, S., Kostrychenko, V., and Koval, V. (2022). Renovation management of the national economy in ensuring energy decentralization. *Polityka Energetyczna – Energy Policy Journal*, 25(2), pp. 67–84. Available at: <https://epj.min-pan.krakow.pl/Renovation-management-of-the-national-economy-in-ensuring-energy-decentralization,150483,0,2.html>

12. Borodina, O. A., Lyashenko V. I., Lishchuk O. V. (2022). Tax on withdrawn capital as a special regime for stimulating reinvestment in industrial parks of post-war Ukraine. *EVD: scientific journal*. Kyiv–Poltava: IEP NASU. No. 3(69), 2022. P.108–123.

13. Regulski, J. (2017). Reformowanie państwa: moje doświadczenia. Szczecin : Wyższa Szkoła Administracji Publicznej. 180 s.

14. Благун І. Г. (2017). Бюджетне фінансування соціальних видатків в умовах макрофінансової нестабільності національної економіки. Розвиток економіки України: трансформації та інновації: монографія : у 2 т. / І. Г. Благун, В. І. Кіт, І. С. Козій; за заг. ред. О. Л. Гальцової. Запоріжжя: Гельветика. Т. 1. С. 100–115.

15. Czym jest estoński CIT i komu przysługuje? Available at: <https://podatki.gazetaprawna.pl/artykuly/8076597.cit-estonski-co-to-jest-na-czym-polega-podatek-w-polsce.html>

16. The World Bank. Countries and Economies. [Electronic resource]. Available at: <https://data.worldbank.org/country>

Section 5

Digital Transformation of Global Security

Chapter 22
***The impact of digitalization on the competitiveness of
Ukrainian businesses in the EU market: challenges and
opportunities***
(D. Bedrii, I. Yatskevych)

The modern economy is characterized by the rapid development of digital technologies, which are changing approaches to doing business and creating new opportunities for international integration. Ukrainian companies seeking to expand their presence in the European Union (EU) market face a number of challenges related to digitalization. This chapter will examine the impact of digital technologies on the competitiveness of Ukrainian businesses, the challenges and opportunities arising in the process of integration into the EU market, as well as state policy and support for digitalization in Ukraine.

The purpose of this chapter is to explore these issues.

22.1. Digitalization as a factor of competitiveness

In the current context of globalization and rapid technological change, digitalization is becoming an important factor in ensuring the competitiveness of companies. It encompasses the process of introducing digital technologies into all areas of activity, from production and logistics to marketing, human resources management, and communications. Digitalization not only changes the organizational structure of companies, but also shapes a new business paradigm based on data, innovation, and flexibility.

In recent years, digitalization has become systemic in Ukraine and has become one of the key factors in the modernization of the economy, public administration, and the social sphere. In the context of war, global instability, and structural changes, digital technologies play a special role in ensuring

economic stability and the continuity of business and government institutions.

As of early 2025, internet penetration in Ukraine stands at around 82.4% of the population, which corresponds to almost 31.5 million users. The number of active mobile connections exceeds 56 million, which means that on average there are more than 1.4 mobile numbers per citizen (Table 22.1) [1]. These figures indicate a high level of access to digital technologies and communication services among the population.

Table 22.1

Key indicators of digitalization in Ukraine*

Indicator	Value / trend
Internet penetration	Approximately 82.4% of the population by early 2025
Number of Internet users	31.5 million people
Number of mobile connections	56.4 million active connections
Share of the IT sector in the economy	~ 3.4% of GDP in 2024
Exports of IT services	Up to 5% of GDP, up to \$7.3 billion in 2023
Business digitalisation index	Average level – 55.7 out of 100
Access distribution in rural areas	Fixed Internet in rural areas increased by 25.4%
Decrease in the use of electronic government services	From ~ 64% in 2023 to ~ 55% in 2024
Network readiness index ranking	Ukraine ranks 43rd out of 134 countries (NRI 2023)

** Source: compiled by the authors based on [1, 2]*

The digitalization of Ukraine’s economy is largely driven by the development of the IT industry, which has become one of the most dynamic sectors of the national economy. In 2024, IT accounted for about 3.4% of the country’s GDP, and IT services exports exceeded 7.3 billion U.S. dollars. Ukraine ranks among the leaders in Europe in terms of the number of highly qualified software developers, startups, and outsourcing companies [2].

The development of digital technologies in business is also gaining momentum: according to estimates by the Kyiv GovTech Centre [3], the average level of digitalisation of enterprises is 55.7 out of 100 points. This indicates a gradual transition from traditional business models to integrated digital solutions – the introduction of CRM and ERP systems, cloud technologies, electronic payments, and online sales platforms.

One of the most notable trends in recent years has been the expansion of digital infrastructure in rural areas. According to data [4, 5], the level of

access to fixed Internet in rural areas has increased by 25.4%, which has significantly reduced the 'igital divide' between urban and rural areas. This was made possible by government programs to develop broadband Internet and the support of international partners.

Ukraine has become one of the leaders in the digital transformation of the public sector. Thanks to the implementation of the Diia ecosystem, the country ranked first in the world in the E-Participation Index and 30th in the E-Government Development Index [4, 5]. Through the Diia mobile app and portal, citizens have access to dozens of administrative services, electronic documents, certificates, and business opportunities.

At the same time, according to data [3], the use of electronic government services has declined slightly, from 64% in 2023 to 55% in 2024. This may be due to the war, restrictions on internet access in some regions, and temporary technical difficulties.

According to the global Network Readiness Index [5], Ukraine ranked 43rd among 134 countries, improving its performance in the areas of 'Human Capital' and 'Technological Infrastructure'. This indicates steady growth in the potential of the digital economy and convergence with average European standards of digital maturity.

Ukraine is undergoing an active digital transformation that is gradually encompassing all areas of public life. The main achievements are a high level of internet penetration, strong development of the IT sector, the spread of public digital services, and the growth of digital literacy among the population.

At the same time, challenges remain: uneven access to the Internet between regions, insufficient cybersecurity, and the need to update the legislative framework. However, current trends indicate that digitalization in Ukraine is becoming the foundation for increasing competitiveness, attracting investment, and integrating into the global digital space.

Digitalization is a complex process of transition from traditional management methods to digital formats based on the use of information and communication technologies (ICT), cloud solutions, Artificial Intelligence (AI), Big Data, and Internet of Things (IoT) technologies. Thus, digitalization involves the integration of digital systems into production, management, and analytical processes to improve efficiency, transparency, and speed of decision-making.

In this context, digitalization is seen not only as a technical upgrade, but as a strategic development tool that allows companies to increase

productivity, reduce costs, create added value based on digital innovations, and strengthen their competitive position in the European market.

By integrating digital technologies into their production, management, and communication processes, Ukrainian companies are able to adapt their business models to EU standards, increasing transparency, energy efficiency, and compliance with sustainable development principles, which are key criteria for participation in joint programs, tenders, and EU supply chains.

Thus, digitalization is becoming a prerequisite for the integration of Ukrainian companies into the European economic space, promoting their innovative growth, international cooperation, and attracting investments from EU countries.

The competitiveness of a modern company is determined not only by the quality of its products or price levels, but also by its ability to quickly adapt to changes in the market environment. It is digital technologies that create the conditions for a flexible response to the challenges of the times.

First, digitalization allows for deep optimization of business processes through automation and integration of key management functions. The use of modern ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), and SCM (Supply Chain Management) systems ensures effective management of the company's financial, human, and material resources. Such tools not only reduce operational management costs but also increase planning accuracy, data processing speed, and process transparency.

This, in turn, contributes to increased resource efficiency, improved cost control, and reduced management decision-making time. Automation of document flow, inventory management, sales analytics, and logistics chains creates the basis for the transition to a 'smart enterprise' model capable of responding flexibly to changes in supply and demand.

Second, digitalization contributes to increased customer focus, which is a key factor in the competitiveness of modern business. Thanks to Big Data analytics, companies can not only track market trends but also predict consumer behavior. The use of machine learning algorithms makes it possible to create personalized offers, customize communications with customers in real time, and increase customer satisfaction.

Social networks, chat bots, and omnichannel marketing platforms create new formats for interaction between companies and customers, which significantly strengthens loyalty and trust. Thus, digitalization transforms the customer experience from passive interaction into a dynamic communication

ecosystem where the consumer is an active participant in shaping the value of the product.

Third, digitalization significantly enhances a company's innovative potential. The use of AI, machine learning, digital twins, and block chain technologies opens up opportunities for the accelerated creation of new products and services, as well as improving the quality of existing ones. Digital twins allow for the virtual simulation of production or operation processes, which reduces testing costs, while block chain technologies ensure transaction transparency and reliable control over supply chains.

Innovative activity is also supported by the development of digital laboratories and R&D departments that work at the intersection of data, technology, and market trends. As a result, companies are able to implement innovations faster, experiment with new business models, and develop unique competitive advantages.

Fourth, digitalization creates conditions for the development of networked interactions and partner ecosystems. The use of digital platforms such as Building Radar, SAP Business Network, Salesforce, and Microsoft Dynamics 365 enable effective collaboration between suppliers, contractors, customers, and government institutions. Such interaction increases the transparency of transactions, ensures product quality control, and reduces the time spent on contract negotiations.

Companies that integrate digital tools into their activities are able to create synergies between different market participants, forming a single digital space for interaction.

Fifth, digitalization has a positive impact on corporate culture and human resource management. The introduction of HRM systems, online communication platforms, and remote work systems contributes to increased productivity, employee engagement, and the formation of a flexible organizational structure. Companies with a high level of digital maturity demonstrate better performance in terms of adaptation to change, internal communication, and the development of innovative thinking among staff.

It is important to note that digitalization is becoming the foundation of a company's sustainable competitiveness. It not only ensures operational efficiency but also contributes to the creation of strategic advantages – from rapid response to market changes to the ability to predict future trends. The use of digital technologies allows companies to integrate into international supply chains, increase the level of trust from partners, and strengthen their position in the global market.

Based on the above, we note that digitalization transforms business from within, changing not only the technological but also the managerial and cultural architecture of the company. It becomes not just a tool for efficiency, but a strategic basis for innovative development, increased customer focus, and the formation of long-term competitive advantage.

In today's turbulent market conditions, digital platforms serve as a strategic basis for coordinating business processes, forming a unified ecosystem of interaction between all market participants-manufacturers, suppliers, customers, logistics operators, financial institutions, and even government agencies. Their key function is to create an integrated digital space where information is exchanged, decisions are coordinated, and actions are synchronized between partners in real time.

Digital platforms allow previously fragmented business processes to be combined into a single network, which significantly increases the efficiency of operational activities. Instead of the traditional sequential interaction between participants in the chain, a digital feedback model is created, where information about demand, supply, inventory, and product quality is updated instantly. This minimizes time delays, reduces errors, and allows for quick responses to changes in market conditions.

One of the main results of the functioning of digital platforms is a reduction in transaction costs, costs associated with finding partners, concluding agreements, monitoring the fulfillment of obligations, and transferring information. Whereas coordination previously required significant administrative and communication resources, platforms now automate these processes. For example, in the construction, logistics, or industrial sectors, such systems allow you to automatically generate orders, check the availability of materials, coordinate delivery schedules, and avoid duplication of costs.

Parallel to the development of platforms, the role of digital risk management tools is growing. In today's fast-changing economy, the ability to anticipate potential threats and respond quickly is critical. Risk management systems based on Big Data, predictive modeling, and AI enable companies to identify risks at an early stage and develop preventive measures (Table 22.2).

Such systems analyze a wide range of data: financial indicators, production trends, market fluctuations, consumer behavior, supplier status, etc. As a result, an integrated risk map of the company is formed, which

allows managers to make informed decisions regarding financing, logistics, marketing, and the development of new projects.

Table 22.2

Interconnection between digital platforms and risk management systems*

Industry	Digital platforms and tools	Risk management functions	Expected effect / Examples of application
Construction	Building Radar, PlanRadar, Autodesk Construction Cloud, BIM 360	– real-time project monitoring – forecasting delivery delays; – control of costs and technical risks	– 10–15% cost reduction; – reduction of project implementation times; – transparency in relations between contractors and customers
Industry (manufacturing)	Siemens MindSphere, GE Predix, SAP Digital Manufacturing Cloud	– detection of malfunctions in production lines; – analysis of equipment condition; – inventory and product quality management	– accident prevention; – reduction of downtime; – optimisation of resources and materials
Agribusiness	Cropio, OneSoil, EOS Data Analytics	– analysis of climatic, agronomic and logistical risks; – Yield forecasting – monitoring of field conditions via satellites	– reduction of crop losses; – effective agricultural production planning; – minimisation of environmental risks
Financial sector	SAP GRC, Oracle Risk Management Cloud, Fadata, SAS Risk Management	– analysis of credit, currency and operational risks; – fraud detection; – liquidity forecasting	– strengthening financial stability; – reducing the likelihood of insolvency; – increasing investor confidence
IT and digital services	Jira, ServiceNow, Azure DevOps, Trello, RiskWatch	– risk management in a project environment; – continuous monitoring of cyber threats; – software development quality control	– improving data security; – acceleration of the development life cycle; – reduction of incident costs

Table 22.2 (continued)

Logistics and transport	SAP Logistics Cloud, Trans.eu, Uber Freight, Project44	– forecasting transport delays; – risk analysis in supply chains; – control of routing and fuel costs	– 8–12% cost reduction; – improved delivery accuracy; – optimisation of logistics flows
Healthcare	Medstar, Helsi.me, Microsoft Cloud for Healthcare	– medical data management; – control of risks to personal information security; – monitoring the effectiveness of treatment	– reduction of diagnostic errors; – improving the availability of services; – secure storage of patient data

**Source: compiled by the authors*

It is particularly important that digital risk management systems ensure a rapid response to crisis situations. In the event of unforeseen events, such as supply disruptions, exchange rate fluctuations, or cyber-attacks, the system automatically alerts the responsible departments, proposing scenarios for action based on preliminary analysis. This allows the company to minimize the impact of crises and maintain operational stability.

Thus, digitalization transforms risk management from a reactive process (responding to an event after it occurs) into a preventive system of forecasting and adaptation. This reduces uncertainty, improves the quality of management decisions, and strengthens the company's financial stability.

Digital platforms and risk management systems form the intellectual framework of modern business. They enable companies to act faster, anticipate challenges, build trust with partners, and achieve sustainable development in a global competitive environment.

Today, digital technologies are seen not only as a tool for improving business efficiency, but also as a system-building factor for sustainable economic growth. They are changing the paradigm of how the economy works, ensuring the rational use of resources, improving energy efficiency, and creating conditions for the development of environmentally responsible production.

In a global context, digitalization is one of the key areas for implementing the UN Sustainable Development Goals [6], as it contributes to the formation of an innovative, inclusive, and 'green' economy. Digital solutions enable companies to reduce energy consumption through process automation and real-time cost monitoring.

As a result of the active introduction of digital technologies, a new model of economic development is emerging – the ‘green economy’, which is based on the principles of sustainability, energy efficiency, and rational use of resources [7]. Unlike traditional approaches, which focused primarily on increasing production volumes, the ‘green economy’ seeks to strike a balance between economic, social, and environmental goals, minimizing the negative impact of human activity on the environment.

At the same time, digital technologies contribute to the development of renewable energy. Smart grids, smart meters, and demand management systems make it possible to balance electricity consumption, integrate green sources – solar, wind, bioenergy – and increase the resilience of the energy system. In agriculture, precision farming solutions are becoming more widespread, using satellite data and sensors to reduce the use of water, pesticides, and fertilizers.

In transportation, digitalization is driving the development of smart mobility: navigation systems, e-tickets, ride-sharing apps, and electric vehicle services are reducing emissions, optimizing traffic, and cutting down on time spent on the road. Digital technologies are also driving the circular economy, in which waste is seen as a resource that can be reused thanks to innovative technological processes.

Digital platforms for environmental monitoring – state, municipal, and corporate – play a special role in the development of the green economy. They combine data from various sources (sensors, satellites, enterprises, public organizations) and provide analytical information for management decision-making. Systems such as EcoCity, OpenDataBot, and GreenDataHub ensure the transparency of environmental indicators and promote public control and business accountability.

The use of Big Data, AI, Cloud Computing, and Blockchain ensures transparency of business processes, control of environmental indicators, and accountability of companies to society [8]. Thus, digitalization acts as a catalyst not only for technological but also for socio-economic change, as it reduces environmental impact, stimulates ‘green’ innovation, and shapes a culture of responsible consumption.

For Ukraine, digitalization has a dual significance. First, it is a tool for modernizing companies and public administration, allowing a transition from outdated administrative practices to open, transparent, and customer-oriented models of interaction. Second, it is the key to integration into the European

economic space, which requires compliance with the principles of the EU's digital, competitive, and sustainable economy.

As part of the state policy of digital transformation, a number of programs are being implemented to create a favorable environment for the development of digital entrepreneurship. In particular, the Diia.Business initiative serves as a platform for supporting companies and start-ups, offering consultations, educational courses, business simulators, and online services for starting, running, and scaling a business [9]. This project has become an example of the successful combination of state support, private initiatives, and digital tools for the development of small and medium-sized enterprises.

Another important area is the introduction of the 'E-residency' regime, which allows foreign citizens to remotely register a business in Ukraine, pay taxes online, and use financial services without being physically present [10]. This not only increases Ukraine's attractiveness to foreign investors, but also expands the integration opportunities of the Ukrainian economy into the global digital ecosystem.

State digital platforms aimed at automating administrative processes and creating open data also play an important role. The introduction of electronic registries, online access to licenses, tender platforms, and digital document management increases the level of trust between business and the state. This contributes to reducing corruption risks, improving the investment climate, and raising Ukraine's international rating in terms of transparency.

In addition, digitalisation opens up new opportunities for the development of green start-ups and attracting international funding through Horizon Europe, EU4Environment, Digital Europe and other programmes [11]. The participation of Ukrainian companies in these initiatives allows for the implementation of environmentally-oriented technologies – from energy management to waste recycling – in accordance with EU standards.

Thus, digitalization is becoming not only a technical but also a socio-economic phenomenon that is transforming approaches to production, management and consumption. It creates the basis for the ecological modernization of industry, energy and urban management, forming the preconditions for the transition to a 'smart' and sustainable economy of the future.

For Ukraine, digitalization is a strategic path to sustainable development and integration into the European digital market. Its successful implementation ensures a balance between economic growth, environmental

responsibility and social progress. It is digital technologies that are becoming the driving force that allows the country to combine innovation, competitiveness, and European values in a single model of a 'smart' state.

Thus, digitalization is a key factor in a company's competitiveness in the modern economy. It ensures flexibility, efficiency, customer focus, and innovation in business. Companies that integrate digital technologies into their development strategy in a timely manner not only reap short-term benefits but also build long-term competitive advantages in the global market.

22.2. The impact of digitalization on Ukrainian businesses entering the EU market

The current stage of Ukraine's economic development is characterized by active integration into the European space, accompanied by the digital transformation of business processes. Digitalization is a key factor in increasing the competitiveness of Ukrainian companies and, at the same time, an effective tool for their entry into the EU market. It ensures technological modernization, increases management efficiency, expands communication channels, and creates conditions for transparent interaction with international partners.

To enter the EU market, Ukrainian companies must meet high standards for product quality, transparency of operations, corporate governance, and sustainable development. Digital technologies are what enable them to achieve this level.

Digitalization creates a unified information space between manufacturers, suppliers, and consumers, which facilitates the integration of Ukrainian businesses into European production chains.

In particular, the implementation of ERP and CRM systems allows Ukrainian companies to keep records in accordance with European standards, optimize logistics, increase customer focus, and manage resources effectively. The use of electronic document management and digital signatures simplifies international communication, reduces time costs, and minimizes the risks of bureaucratic barriers.

Digitalization is particularly important for small and medium-sized enterprises (SMEs), which form the foundation of the Ukrainian economy. Today, this sector accounts for over 99% of all businesses in Ukraine, provides about 74% of jobs, and generates over 55% of the country's gross domestic product (GDP) [12, 13]. It is SMEs that form the basis of the

national business environment, influence employment, regional development, and the competitiveness of the economy as a whole.

In today's environment, digitalization is becoming a decisive factor in the survival and development of SMEs, as it enables businesses to respond effectively to market challenges, increase productivity, and expand beyond local markets. For small businesses, which often have limited financial, human, and technical resources, digital technologies open up new opportunities for development – from creating online stores to using AI for sales or consumer behavior analytics (Table 22.3).

Thanks to digital solutions, entrepreneurs gain access to new sales channels, can work remotely, communicate with customers through social networks, optimize operational processes using CRM and ERP systems, and automate accounting, document management, and logistics. Such tools not only increase management efficiency but also reduce administrative costs, allowing owners to focus on strategic business development.

Digitalization also contributes to greater transparency in the activities of SMEs, which is particularly important in the context of Ukraine's integration into the European economic space.

The use of electronic document management, digital signatures, open databases, and online reporting strengthens trust between entrepreneurs, partners, and government agencies. This facilitates the participation of small businesses in tenders, international contracts, and EU investment programs such as EU4Business, Horizon Europe, COSME, and Digital Europe.

In the context of war, digital tools have become a means of adapting businesses to crisis conditions. Many small companies have been able to stay in business by moving online: e-commerce, remote consulting, online education, freelance platforms, and logistics services have helped companies retain customers and ensure business continuity.

According to data [12; 13], more than 40% of SMEs in 2023-2024 have partially or completely transitioned to a digital environment, which has become one of the key factors in their resilience.

At the same time, the level of digital maturity of small businesses remains uneven. In large cities, about 90% of companies have access to high-speed Internet, while in rural communities this figure is only about 65%. This indicates the need for state support in the form of digital education programs, investments in digital infrastructure, and the provision of preferential loans for the implementation of technologies.

Table 22.3

The impact of digitalization on the development of small and medium-sized enterprises in Ukraine*

Impact	Main areas of digitalization	Effects for SMEs	Comments
Economic	Implementation of ERP, CRM, SCM systems, online commerce, electronic document management	– optimisation of business processes and cost reduction; – acceleration of capital turnover; – increasing sales through digital channels	– SMEs account for 55% of GDP – 40% of enterprises have partially or completely moved online; – 60% of SMEs use CRM or online accounting
Social	Use of digital services in the areas of labour, education, communications and services	– creation of new jobs in the digital sector; – flexibility of employment; – reduction of regional differences in access to the labour market	– 74% of jobs are created by SMEs; – more than 200,000 users have completed online training as part of the "Diia.Business" programme; – 28% increase in the number of registered freelancers
Technological	Use of Big Data, IoT, AI, Cloud Computing, cybersecurity	– automation of management processes; – improvement of demand and risk forecasting; – increased business innovation	– 85% of SMEs have access to the Internet; – 50% use cloud services; – growth in the share of online operations in the service sector - up to 65%
Institutional (state)	Business digitalisation support programmes, 'Diia.Business', 'E-residency', EU grants	– simplification of regulation and reduction of administrative burden; – access to international programmes and funding – increased trust between business and the state	– SME development strategy until 2027; – 25 Diia.Business support centres; – 4,000+ registered e-residents
Export and integration	SMEs entering international markets through e-commerce, digital marketing, EU4Business	– expansion of sales geography; – attracting investment	– 17% of SMEs export online; – 9% have partners in the EU

**Source: compiled by the authors based on [12, 13, 14, 15]*

At the state level, SME development and digitalization are combined in the Small and Medium Business Development Strategy until 2027 [16], approved by the Cabinet of Ministers of Ukraine in 2024. The document

defines digital transformation as a priority area of state policy aimed at automating processes, creating online business support services, and improving the digital literacy of companies.

One example of the practical implementation of this policy is the Diia.Business project [9], which provides access to training courses, consultations, business plans, and marketing tools in digital format. Entrepreneurs can also use the Diia platform to register as sole proprietors, obtain permits, file tax returns, and even participate in state funding programs without visiting offices.

Gradually, the digitization of SMEs is becoming an important factor in socio-economic stability: it contributes to the development of local communities, the creation of new jobs, and the expansion of the domestic market. The growth in the number of online entrepreneurs, freelancers, creative agencies, and tech startups shows how small businesses are moving into the digital sector of the economy.

Digitalization is not just a technological trend, but a driving force behind the transformation of small and medium-sized businesses in Ukraine. It paves the way for innovation, increased efficiency, and international integration. Thanks to digital tools, SMEs are becoming more flexible, competitive, and resilient to crisis challenges, and thus key players in building Ukraine's modern digital economy.

The entry of Ukrainian companies into the European Union market requires not only technological modernization but also systemic trust on the part of European partners. In this context, digitalization is a key factor in ensuring transparency, reliability, and compliance with European business standards. When choosing partners, European companies and investors give preference to companies that ensure digital openness, stable reporting, and compliance with good governance standards.

Thanks to digital technologies, Ukrainian businesses have the opportunity to integrate into the European economic space through the harmonization of management, financial, and logistics processes. In particular, the use of data management systems, electronic registries, online reporting, and cloud accounting services allows for a high level of transparency, which is one of the key requirements for companies operating in the EU.

Technologies such as ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), and BI (Business Intelligence) ensure accurate reporting, financial forecasting, and real-time risk management.

They build trust in Ukrainian companies as partners that operate according to the principles of corporate responsibility, stability, and digital discipline.

Digitalization also helps reduce corruption risks and increase business accountability. Thanks to open data, electronic procurement (through the Prozorro system), and digital platforms for public services (Diia, E-Data, Spending.gov.ua), an environment is being created in which interaction between the state, business, and society is becoming more transparent. This creates a favorable backdrop for long-term investment, international partnerships, and the participation of Ukrainian companies in joint European projects.

Another important area is the adaptation of Ukrainian companies to European standards of auditing and financial reporting. The online reporting system and the implementation of IFRS (International Financial Reporting Standards) and ESRS (European Sustainability Reporting Standards) allow companies to be understood by European banks, funds, and institutions. Such transparency is an important condition for attracting funding under the EU4Business, Horizon Europe, Digital Europe, and InvestEU programs.

Digital technologies are becoming not only a technical tool for integration, but also a communication bridge between Ukrainian and European businesses. Modern platforms for video conferencing, electronic document management, contract management, and cross-border payments (in particular through SEPA, SWIFT gpi, and e-invoicing) significantly simplify cooperation processes and minimize time and geographical barriers.

An additional strategic aspect of modern digital policy is the implementation of ESG (Environmental, Social, Governance) principles, which are becoming globally important. For EU countries, these criteria are fundamental when making investment decisions and determine a company's reputation. Ukrainian companies that combine digital solutions with environmental and social responsibility gain significant competitive advantages:

1. Environmental component – includes the use of digital tools for monitoring energy consumption, CO₂ emissions, waste management, and environmental certification of products.

2. Social – implemented through the creation of inclusive working conditions, support for remote employment, and improving the digital literacy of staff and customers.

3. Management – consists of the implementation of electronic audit systems, risk analytics, transparent decision-making systems, and digital integrity policies.

Companies that integrate ESG principles into their digital business model not only strengthen their position in the domestic market but also increase their chances of attracting European grants, investments, and partnerships. Within the framework of Ukraine's future accession to the EU, compliance with European ESG and cybersecurity standards will become a prerequisite for participation in the common digital market.

Ukraine's State Strategy for Digital Transformation until 2030 [17] provides for the gradual introduction of EU standards in the areas of e-government, cyber security, personal data protection, and environmental monitoring. Such synchronization contributes to building trust, which is the basis for partnerships between Ukrainian businesses and European corporations, banks, and institutions.

Digitalization is not only a technological investment but also a reputational investment in the future of Ukrainian business. It increases transparency, builds trust, ensures compliance with European standards, and creates conditions for Ukraine's integration into the EU's common digital space. Combined with ESG principles, digital transformation becomes the foundation of a new business culture where success is measured not only by profit but also by responsibility, innovation, and sustainable development.

Digitalization is becoming a key tool for integrating Ukrainian businesses into the European market. It not only optimizes internal processes, but also increases trust, efficiency, and competitiveness among companies.

Thanks to digital technologies, Ukrainian companies have real opportunities to participate in EU cooperation programs, attract investment, expand customer markets, and build a positive brand for 'digital Ukraine'.

The further development of digitalization must be based on state support for innovation, the development of digital education, the creation of a favorable legislative environment, and the development of cyber infrastructure. Only under such conditions will digital transformation become the basis for the sustainable entry of Ukrainian businesses into the European Union market and the strengthening of their positions in the global economy.

22.3. State policy and support for digitalization in Ukraine

In the 21st century, digitalization has become a strategic direction for the development of national economies, and for Ukraine, it is one of the priorities of state policy for modernization and European integration. In the context of global digital transformation, the state plays a key role in creating the legal, organizational, and financial prerequisites for the introduction of digital technologies in all spheres of public life, from the economy and education to public administration and the provision of public services.

State policy in the field of digitalization in Ukraine is based on the Concept for the Development of the Digital Economy and Society for 2018-2020 [18]. The main goal of this document is to create conditions for the establishment of a digital economy, the development of citizens' digital competencies, digital infrastructure, and an innovative business environment.

These provisions were subsequently developed within the framework of the Strategy for Digital Development of Innovation until 2030 [17], which is aimed at ensuring the complete digital transformation of the state, business, and society, as well as integration into a single European digital space.

The main directions for the implementation of state policy are as follows:

1. Digitalization of public administration. One of the most notable achievements is the creation of the 'Diia' ecosystem [19], which provides over 120 electronic services, digital documents, and services for businesses and citizens. Ukraine became the first country in the world where an electronic passport has the same legal force as a paper one.

The Diia.Business portal functions as a tool to support entrepreneurs, providing consultations, online courses, document templates, and market analytics.

2. Development of digital infrastructure. The state is actively investing in the development of broadband Internet access, especially in rural areas. The Internet Subsidy Program [18] has enabled more than 3,000 settlements to be connected to optical networks. The Wi-Fi in Communities project [18] is also being implemented, providing free access to the network in public spaces.

3. Digital education and improving digital literacy. As part of the 'Diia.Digital Education' initiative, an online platform has been created, where more than 1.5 million citizens have already completed training programs in digital literacy, cybersecurity, artificial intelligence, and e-commerce [18]. At

the same time, projects are being implemented to prepare civil servants to work in a digital environment.

4. Support for the digital economy. The introduction of the special legal regime “Diia.City” was a breakthrough in the IT business [9]. It provides preferential tax conditions, simplifies labor relations for specialists, and stimulates the development of innovative startups. In 2025, more than 800 residents joined ‘Diia.City’, including leading Ukrainian and international IT companies.

The state policy of digitalization in Ukraine is not only a technological project but also an institutional reform that encompasses all levels of society. It ensures the openness of government, improves the efficiency of public administration, involves citizens in decision-making, and stimulates the development of the digital economy. In the long term, this creates a foundation for sustainable development, digital democracy, and Ukraine’s deep integration into the European political, economic, and digital space.

In today’s globalized world, digitalization has become not only an internal policy of states but also an instrument of international integration. For Ukraine, international cooperation in the field of digital transformation is of strategic importance, as it determines the possibilities for integration into the global knowledge economy, participation in global innovation chains, and the development of digital services. The European vector of digitalization is one of the most important areas of state policy, contributing to Ukraine's rapprochement with the European Union not only politically, but also technologically, institutionally, and normatively.

After receiving EU candidate status in 2022, Ukraine began to gradually harmonize its digital legislation with European legislation. At the heart of this process is the implementation of the principles of the EU’s digital single market, which provides for the free movement of data, access to digital services, and uniform standards for security and personal information protection. The compliance of Ukrainian digital policy with European requirements in areas such as cybersecurity, e-commerce, digital identifiers, cloud services, and AI is a guarantee of further economic and political convergence.

Ukraine’s participation in the EU’s Digital Europe Program is of particular importance. This initiative aims to increase the digital competitiveness of participating countries and support key technologies, including artificial intelligence, computing power, cybersecurity, and digital

skills. Ukraine's participation in the program opens up access to funding, knowledge sharing, and participation in joint scientific and technical projects.

Another area of cooperation is the EU4Digital program, which focuses on the development of e-commerce, digital logistics, electronic trust services, and cross-border data exchange. Ukraine is actively working to join the European electronic signature system, which will allow Ukrainian electronic documents to be legally recognized in EU countries. This will greatly simplify international business, participation in tenders, and open up new opportunities for digital companies.

Cooperation within the Horizon Europe, Erasmus+, EU4Innovation, and Creative Europe programs plays an important role in education and research. These programs promote the development of digital skills, an innovative ecosystem, startups, and academic mobility. Ukrainian universities, technology parks, and IT companies participate in joint projects that promote integration into the European scientific and technological space.

The European vector of digitalization also involves the development of cross-border cooperation, especially in the field of smart infrastructure – transport, energy and communications. Ukraine's participation in the Trans-European Transport Network and Energy Community initiatives enables the implementation of digital technologies for monitoring, automated management and resource optimization. Such solutions strengthen energy and logistics security, increase transport efficiency, and reduce environmental impact.

An important aspect is cooperation in the field of cybersecurity, which is particularly important in the context of military aggression against Ukraine. Thanks to partnerships with the European Network and Information Security Agency, NATO, and the G7 countries, Ukraine is strengthening the protection of critical digital infrastructure, developing early detection systems for cyberattacks, and forming a cyber resilience strategy at the state level.

International financial organizations provide significant support for digital reforms. The World Bank, the European Bank for Reconstruction and Development, and the European Investment Bank are implementing programs to finance e-governance, digital education, the development of Internet infrastructure in the regions, and the creation of secure data centers. These projects contribute to the modernization of public administration, the development of small and medium-sized businesses, and the promotion of digital inclusion.

An equally important component of international cooperation is Ukraine's participation in global initiatives of the UN, OECD, ITU, and World Economic Forum related to sustainable development, open data, digital ethics, and artificial intelligence regulation. Ukraine is gradually joining the development of international standards for digital governance, which will help strengthen its position as a regional digital hub in Eastern Europe.

Based on the above, we can identify the main areas of Ukraine's international cooperation in the field of digitalization (Table 22.4).

Thus, international cooperation in the field of digitalization is a systemic factor in Ukraine's European integration. It not only provides access to innovation, finance and technology, but also contributes to the formation of a new model of interaction between the state, business and civil society.

In the long term, the implementation of the European digitalization vector will contribute to the creation of a single Ukraine-EU digital space, which will become the basis for sustainable development, competitiveness, and Ukraine's full membership in the European Union.

Despite significant achievements, the implementation of the state digitalization policy faces a number of challenges:

- digital inequality between regions;
- a shortage of IT specialists in the public sector;
- cybersecurity threats due to war and hybrid attacks;
- slow adaptation of legislation to the pace of technological development.

The state policy of digitalization in Ukraine is comprehensive and covers all aspects of social development, from digital governance to support for innovative businesses. Thanks to the implementation of strategic programs such as Diia, Diia.City, Diia.Business, and Digital Education, Ukraine has become an example of rapid digital transformation even in the difficult conditions of wartime.

The further success of digitalization depends on the coordination of government, business, and educational initiatives, harmonization with EU legislation, and maintaining the investment attractiveness of the IT sector. In the long term, Ukraine's digital policy should become the basis not only for technological but also institutional integration into the European digital space, strengthening the state's position in the global knowledge economy.

Table 22.4

Main areas of Ukraine's international cooperation in the field of digitalization*

Area of cooperation	Partner organizations / Programmes	Key results and initiatives	Expected effects for Ukraine
European digital market	European Commission, DG CONNECT, European Council	– harmonisation of legislation with eIDAS and GDPR regulations; – development of electronic trust services; – integration into the cross-border data exchange system	– recognition of Ukrainian electronic signatures in the EU; – simplification of business interaction with European companies
Digital Europe Programme	EU, Ministry of Digital Transformation, EIB	– participation in grants for AI, Cloud, HPC, cyber security; – support for Ukrainian IT companies and start-ups	– attracting investment in the digital economy – improving the country's technological capabilities
EU4Digital programme	EU, EBRD, Eastern Partnership	– development of e-commerce and logistics; – introduction of cross-border eDelivery and eSignature; – development of 5G infrastructure	– expansion of the digital services market; – increasing exports of IT products
Horizon Europe and Erasmus	EU, European Commission, Ukrainian universities	– joint research in the field of digital innovation; – support for STEM education and start-ups; – academic mobility	– strengthening innovation capacity; – improving the digital competence of specialists
EU4Business and COSME programmes	EU, Ministry of Economy of Ukraine, EBRD	– support for SMEs through digital tools; – grants for automation and online promotion; – training programmers' on digital literacy	– increasing the competitiveness of SMEs; – integration of businesses into the EU market
Cybersecurity and infrastructure resilience	NATO, ENISA, USAID, Cyber Sec4 Europe	– development of a national cyber defense system; – development of CERT-UA and data exchange with the EU; – training programmers on cyber hygiene	– improving the security of critical infrastructure; – reduction of the risk of cyber attacks

Table 22.4 (continued)

E-government and open data	World Bank, UNDP, OECD	– development of the Diia platform – opening of state registers; – automation of public services	– reduction of corruption risks; – transparency of public administration
Infrastructure and digital networks	ITU, EIB, Cisco, Nokia, Huawei	– development of 4G/5G coverage; – projects involving digital hubs and data centres; – development of high-speed internet in communities	– expansion of access to digital services; – increasing the level of digital inclusion
Environmental and sustainable digital technologies (ESG)	UNDP, OECD, Green Digital Coalition	– implementation of green IT solutions; – development of digital monitoring of environmental data; – ESG reporting in companies	– strengthening international reputation; – access to EU green investments
Humanitarian and social digitalisation	UNICEF, UNESCO, GIZ	– digital education programmes – support for online educational platforms; – development of digital inclusion for IDPs	– improving digital literacy among the population; – inclusive regional development

* Source: compiled by the authors

Digitalization is one of the main factors influencing the competitiveness of Ukrainian businesses in the EU market. While companies face challenges such as regulatory barriers, cybersecurity, and the need for significant investment, digital technologies open up vast opportunities for international integration and growth. Joint efforts by the state, business, and international partners will help accelerate digital transformation and strengthen Ukraine's position in the global economy.

References

1. Digital 2025: Ukraine. Available at: <https://datareportal.com/reports/digital-2025-ukraine>
2. Інтернет, соцмережі, стримінги та відео. Найцікавіше зі звіту Digital 2025 про взаємодію з цифровими технологіями. Available at:

<https://mediamaker.me/najczikavishe-zi-zvitu-digital-2025-pro-vzayemoDiiu-z-czyfrovymy-tehnologiyamy-16257>

3. Ukraine's GovTech Topping Global Rankings. Available at: <https://digitalstate.gov.ua/news/govtech/ukraines-govtech-topping-global-rankings>

4. State Digital Transformation in Ukraine: 2019–2024 Review. Available at: <https://voxukraine.org/en/state-digital-transformation-in-ukraine-2019-2024-review>

5. How Ukraine's Business Digitalization Is Measured. Available at: https://www.kyivgovtechcentre.org/report_on_the_level_of_business_digitalization_in_ukraine_published

6. 17 Цілей сталого розвитку. Available at: <https://globalcompact.org.ua/tsili-stijkogo-rozvytku/>

7. Поліщук, Ю. (2021). Концепції державної політики розвитку “зеленої” економіки: еволюція, сутність, цілі та принципи. Ефективність державного управління. Вип. 65. С. 207–218. <https://doi.org/10.33990/2070-4011.65.2020.226476>

8. Yatskevych, I., Bedrii, D. (2025) Digital transformation as a tool for sustainable spatial development of ukraine's regions: challenges, prospects, indicators. International scientific journal «Grail of Science». № 51. С. 260–267. <https://doi.org/10.36074/grail-of-science.18.04.2025.032>

9. Дія.Бізнес Старт. Available at: <https://business.diiu.gov.ua/>

10. uResidency: в Україні стартує програма електронного резидентства для іноземців. Available at: <https://business.diiu.gov.ua/news/uresidency-v-ukraini-startuie-prohrama-elektronnoho-rezydentstva-dlia-inozemtsiv>

11. Horizon Europe, EU4Environment, Digital Europe. Available at: <https://digital-strategy.ec.europa.eu/en/activities/digital-programme>

12. Результати дослідження стану бізнесу в Україні у березні 2025 року. Available at: <https://business.diiu.gov.ua/analytics/research/rezultaty-doslidzhennia-stanu-biznesu-v-ukraini-v-berezni-2025-roku/>

13. Державна служба статистики України. Available at: <https://www.ukrstat.gov.ua>

14. Rychlik, A., Semko, O., Bedrii, D., Marshak, O., Nesterenko, A. (2024). Information System for Management of Information Risks in Digital Transformation Projects. Information Technology for Education, Science, and Technics. ITEST 2024. Lecture Notes on Data Engineering and

Communications Technologies. Vol. 222. P. 3–17.
https://doi.org/10.1007/978-3-031-71804-5_1

15. Chernenko, Yu., Bedrii, D., Haidaienko, O., Meliksetov, O. (2025). Mitigating operational risks in critical infrastructure through integrated ERP-BPMS: a multi-case study. *Technology Audit and Production Reserves*. № 3 (4(83)). P. 53–63. <https://doi.org/10.15587/2706-5448.2025.330660>

16. Уряд схвалив Стратегію розвитку малого та середнього бізнесу до 2027 року та операційний план заходів на 2024-2027 роки. Урядовий портал. Available at: <https://www.kmu.gov.ua/news/uriad-skhvalyv-stratehiu-rozvytku-maloho-ta-serednoho-biznesu-do-2027-roku-ta-operatsiinyi-plan-zakhodiv-na-2024-2027-roky>

17. WINWIN: Україна затвердила Стратегію цифрового розвитку інновацій до 2030 року. Міністерство цифрової трансформації України. Available at: <https://thedigital.gov.ua/news/technologies/winwin-ukraina-zatverdila-strategiyu-tsifrovogo-rozvitku-innovatsiy-do-2030-roku>

18. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації. Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. Available at: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>

19. Дія. Державні послуги онлайн. Available at: <https://diia.gov.ua/>

20. Програма ЄС «Цифрова Європа» (2021-2027). Available at: https://business.diia.gov.ua/finance/program/programa_es_cifrova_evropa_2021_2027

Chapter 23

The impact of digitalization risks on the formation of the human resource potential of enterprises of the region and it's reflection in their development management strategies ***(N. Zachosova)***

An important characteristic of human capital and intellectual potential of modern business entities is the digital literacy of personnel and the level of development of their social skills. However, digitalization brings both advantages and new opportunities for business, as well as threats. And only its employees and top management are able to turn the risk of digitalization into a new competitive advantage for the company, who, with the help of their knowledge and skills, using digital technologies, create new intangible assets necessary for the strategic and sustainable development of enterprises. However, it is not easy for managers to motivate performers to professional improvement, because there are fears in teams and teams that automation and artificial intelligence will soon completely replace the work of personnel performing routine functions. Such alternatives – competitive advantages versus resistance to change, experience and professionalism acquired over the years – versus artificial intelligence, personal communication and interaction – versus instant information exchange – actualize the need to find rational management solutions to take into account the impact of digitalization risks on the formation of the human resource potential of enterprises in the region in the strategies for managing their development.

The study of these issues is the purpose of this chapter.

23.1. The role of human resources in the strategic development of enterprises

The human resource potential of an enterprise in the general sense of this term is a set of knowledge, skills and abilities of its employees, which they can and are ready to use when performing their professional duties, and is also considered a systemic characteristic of its human resource as a whole, which combines the assessment of such qualitative and quantitative parameters as the acquired professional experience, innate abilities (for example, for quick learning, barrier-free communication, etc.), talents, levels of motivation, creativity and loyalty of employees, their readiness and ability to develop their natural abilities and competencies obtained during professional employment. The presence of such qualities in the staff determines its readiness and ability to move towards ambitious strategic goals that the company defines in its strategies, the ability to adapt to changes that are necessary for the transition of the business entity from its current financial and economic state to the desired state, in accordance with the outlined strategic guidelines for long-term development.

The topic of researching the impact of human resources and approaches to personnel management, including under the influence of digitalization risks and other threats to business functioning, is widely studied in the publications of modern Ukrainian scientists. Let us outline the most popular aspects that have gained significant publicity in professional articles by Ukrainian researchers. For example, Voronka O. Z. focuses on the formation of tactics and strategies for ensuring the personnel security of an enterprise [1], Dykan O.V., Kosintseva P.Yu. study the features of personnel security in the process of managing strategic changes [2], Dyachkov D. V., Bohdan M. O., Vovkovynsky Y. V. specify the essence and role of managing the personnel security of an enterprise in the conditions of digitalization of the business environment [3], Zhukovska V. M. summarizes the digital challenges of personnel security of an enterprise [4], Kotelevets D. traces the trends in personnel security of Ukrainian enterprises in the conditions of the digital economy [5], Mishchenko V. I. focuses on the aspect of ensuring the sustainability of the human resource potential of an enterprise in the conditions of digitalization [6], Nizhegorodtsev V., Petrenko L. critically assess the digital tools of the human resource component of the system of economic security of an enterprise [7], Pavlykyvska O. I., Halinyak L. O. support the importance of strategic provision of human resource potential of

enterprises with arguments [8], Rekun G. P., Medenets V. V. make a transition from the micro to the meso level of research into management problems, and propose a mechanism for managing strategic gaps in human resource provision for the development of the region [9], Rudzik D. S. tracks the features of the development of human resource potential of public administration in the conditions of digitalization of society [10], Slatvinsky M. A. studies new opportunities in the development of human resource potential of organizations through the use of digital educational platforms [11], Tokmakova I. V., Korin M. V., Polozov A. E., Avagimova V. A. analyse the problems of personnel support for innovative and digital modernization of enterprises [12], Chernikova N. M. also investigates the problems of personnel support for enterprises in the context of digital transformations [13], Chorna L. O., Kudlayenko S. V., Chorna N. Yu., Kelmanovych O. describe personnel management and its technical and technological support as a component of operational and strategic management of organizations [14], Prykhodko L. S., Bilous S. P. investigate the tools for managing the communication policy of a business entity for the purpose of ensuring its personnel security and achieving strategic development goals [15], Halinyak L., Spivak S., Marynyak B. substantiate the feasibility of developing a personnel support strategy as an element of the educational potential of an enterprise [16], etc. Content analysis of the listed publications allowed us to conclude that the issues of personnel management and development of human resources potential of modern enterprises should be addressed in wartime with an emphasis on ensuring personnel security, as well as taking into account global trends in the development of entrepreneurship, such as digitalization and digital transformation of financial and economic systems and business processes.

Let us outline the role of human resources for the strategic development of enterprises.

The functional goals of the enterprise in various areas of its activity - financial, information, investment, market, etc., are recorded in its strategy of functioning or development. Thus, the strategy of a business entity in practice is a document that specifies its mission, vision and goals of existence, reveals the possibilities of influencing the market and its participants, specifies long-term guidelines for continuing financial and economic activity under the influence of risks in the long term. The strategy, as a management information resource, can have a different structure, an unlimited number of sections and subsections, however, during its development it is worth considering that a

concise and clear presentation of information simplifies the perception and understanding by the company's management of their priority tasks and challenges on the way to the expected qualitative changes and forecast indicators and contributes to the rapid adoption of strategic management decisions.

To streamline the processes related to search, recruitment, onboarding, adaptation, motivation and control of personnel, HR specialists develop and agree with the company's management its personnel strategy. In the future, the main vectors of the formation and development of the company's human resources are determined by its personnel policy, which describes and explains what course in personnel management should be followed to successfully achieve the goals of the personnel strategy. The presence of such documents in the business entity is evidence of its attempts to establish human-centered management and create comfortable working conditions to preserve human resources and form a personnel reserve. Therefore, at the theoretical and methodological level of management science, personnel policy is perceived as a system of views and principles in a holistic personnel strategy through the formulation of a highly productive, cohesive personnel potential for the effective achievement of the goals and objectives of the enterprise, as a set of directions for implementing the personnel strategy, and the personnel strategy is perceived as a document that defines priority personnel goals, a set of organizational decisions and measures, the implementation of which allows achieving the goals of the corporate strategy [8, p.105]. That is, personnel potential is the resource basis of both the personnel strategy and the personnel policy of the enterprise.

Depending on the HR strategy chosen by the company, approaches to the development of human resources and human capital, which forms the basis of its human resources, may be different. If the strategy is aimed at achieving the goals of sustainable business development, then significant attention of the company's HR management is paid to adhering to the principles of human-centered management, ensuring equal access to employment regardless of sex, age, gender, religion of the candidate for the position (strict adherence to the DEI principles), encouraging personnel to use corporate resources economically, constantly developing a social responsibility policy and following the provisions of the concepts of socially oriented management. The priority in the motivational mechanism is given to the timely identification of urgent needs of employees and the search for tools to best meet their interests.

Choosing a strategy to ensure competitiveness and strengthen the influence of the enterprise on the selected market stimulates HR managers to increase the intellectual potential of employees in order to form an intangible reserve to increase the level of competitiveness of the company and achieve leadership in the future in the selected market segment. Such a strategy provides for the presence of a permanent system of training, advanced training, mentoring support and coaching for new employees, periodic comprehensive assessment of their professional characteristics and planning of areas for their development and supplementation with relevant skills and competencies. The HR department or a similar structural unit can set clear requirements for the frequency of improving the level of qualification and the obligation to undergo additional training for the enterprise's employees. The motivational mechanism under such a strategy is focused on recognizing and rewarding those members of the labour collective and project teams who demonstrate the best dynamics in increasing the level and updating their own professional and social skills, capable of providing them with higher labour productivity and the ability to generate innovative ideas in the direction of obtaining additional competitive advantages for the enterprise.

The strategy of safety-oriented management of an enterprise aims at its development taking into account those threats, risks, dangers and challenges that are formed in its external and internal environments and can significantly affect the efficiency of using available or involved resources, or their current functional state. Such a strategy will certainly have clear requirements for personnel, in particular, regarding the basics of their safety-oriented behaviour and the ability to resist threats and transform emerging risks into economic benefits for the enterprise. The lack of the necessary knowledge and experience regarding this form of behaviour makes it necessary to organize training and conduct an information campaign among the enterprise's staff in order to form the basic principles of understanding the rules and policies of safety-oriented management at different levels of functioning of the socio-economic system, which is a classic business entity. The direction of human resource development under such conditions should be the formation of risk management skills, as well as the ability to identify risks and timely inform about their occurrence to persons responsible for managing the financial and economic security of the enterprise. An important role for the effective implementation of such a strategy is played by the ability of employees to communicate, think analytically, and critically assess the situation that has developed in the process of their work and during the

performance of their official duties. In this context, we can talk about the feasibility of additional economic education for key categories of company employees, as well as the active use of legal mechanisms to protect the enterprise's activities from fraudulent and dishonest behaviour of its own employees.

In today's conditions of economic instability and social tension, Ukrainian enterprises are increasingly choosing a passive strategy of activity (not development, but simple economic existence), which focuses on preserving and supporting the achieved indicators of financial condition, such as liquidity, solvency, financial stability, financial independence, etc., competitive positions in the domestic market of goods and services and on preserving the existing human resource without spending additional assets on increasing its intellectual potential. This vision of the company's management is reflected in the fact that employees are not motivated for professional development, but are necessarily tested for their ability to perform their professional duties qualitatively. Therefore, if there is an evolution or technological change in the company's business processes, its management expects employees to independently adapt to it, learn and develop the ability to work in new conditions without additional financial, informational or educational support for this process from management personnel or owners of the enterprise. This approach is not always effective, and works only when employees have a high level of self-motivation for their own professional development. However, if they are not ambitious, and their behaviour is characterized by passivity and total resistance to any changes, their expectations are cautious about the introduction of innovative technologies, etc., the level of loyalty is average or not identified by HR employees, then the risk of bankruptcy and liquidation of the company in the future is quite high, because in the event of the loss of human resources, even of such "low" quality, the passivity of the HR strategy and policy of the business entity will not allow it to recruit new employees in conditions of a shortage of labour supply on the domestic labour market, which arose as a result of a large loss of human capital with the beginning of a full-scale war in Ukraine.

Therefore, the tools for implementing any type of selected HR strategy are HR planning, current HR work, personnel management, measures for its development, advanced training, solving social problems, remuneration and motivation. As a result of the use of these tools, the behaviour of employees

changes, the efficiency of their work increases, and the structure of the team improves [8, p.110].

Thus, the role of human resources for the strategic development of enterprises is:

- production by personnel of new ideas and innovative approaches to solving standard tasks and tasks in conditions of shortage of material and financial resources and under the influence of risks of uncertainty and threats of wartime;
- balanced use by employees of the resource base of the enterprise, taking into account the impossibility of its constant replenishment and the lack of state support for domestic business;
- minimizing the need to search for and attract new employees due to the ability of existing personnel to develop and increase the level of their own qualifications both on the initiative and under the incentives of the company's management, and at their own request;
- adaptation of the behaviour of the labour resource to changing needs and interests of the business entity in accordance with its chosen strategy of functioning and development;
- obtaining by the enterprise competitive advantages and reserves for conducting competitive struggle through the development and use of intangible assets, for example, in the form of intellectual property objects;
- because management personnel act as creators of enterprise development strategies, and therefore the level of their intellectual capabilities, ability and capacity to assess risks and forecast economic trends of the environment in which the company operates significantly determines the achievement of static business development guidelines and the efficiency of using available resources to obtain high economic results.

The constancy of the quality of the human resource, and therefore its potential, may mean for the enterprise the opportunity to remain on the market and satisfy the current needs of consumers, however, it leaves a very low probability of its sustainable development, the realization of the opportunities that its strengths give it, and the counteraction to innovative threats that may appear suddenly, but have fatal consequences for its financial condition, economic security and economic prospects.

Awareness by the enterprise management of the importance of developing its human resource potential can become a catalyst for significant qualitative changes and reorganization of its HR management system and the management model of the business entity as a whole. Since human resources

are an intellectual tool of the company, which initiates the development, implementation and implementation of strategic plans for its development, the constant improvement of the competence of top management and key employees at the levels of the management structure is a necessary condition for the strategic business guidelines to become achievable and can be flexibly changed, if necessary, by employees who have a sufficient level of knowledge, skills and abilities. An important condition for increasing human resources potential is the company's information policy regarding the specification of the role of each employee and his contribution to achieving the strategic goals of the business. For ordinary employees, performers of routine operations, etc., it is very important to feel "noticed" and valuable to the company. Even in the absence of the necessary material resources for an effective motivational policy, verbal praise, public recognition in the team, the provision of an important assignment, for example, servicing a VIP client or conducting a negotiation process, creates in employees a sense of pride and advantage from the privilege of belonging to the team of such an enterprise, the management of which sincerely cares about each employee, knows his needs and tries to satisfy them. Understanding the team role allows a team member to realize what skills, knowledge and abilities he lacks in order to professionally fulfill the duties assigned to him and not let other team members down. The described management and information approach stimulates self-management and the desire of employees for self-improvement and professional growth, and also contributes to saving company resources due to the employee's independent initiative focus on filling with his own strength those 'competence gaps' that are most relevant in the process of his current professional activity and in his predicted 'career future'.

Since the strategic development of an enterprise requires constant updating and supplementing the list of knowledge and competencies of its personnel, the investments that business owners are willing to make in the organization and implementation of the training process for personnel, in the system of improving their qualifications and managing talent development, will allow it to gain significant competitive advantages in the future, as well as acquire the status of a 'training organization', which, in turn, will contribute to the formation of a positive image of the company as an employer and expand opportunities for cooperation with foreign investors and partners who value social initiatives and respect the tendency towards innovation orientation and human-centered management.

23.2. Problems of forming human resources in the regions of Ukraine in wartime conditions

With the beginning of the full-scale invasion, some regions of Ukraine found themselves in the status of occupied territories, some were recognized as front-line territories, where the level of security for doing business and professional activities is quite low, and some regions were recognized as rear and conditionally safe for the existence and activity of companies and the stay of their employees. Therefore, depending on the status, each region of Ukraine now has its own set of problems regarding the formation and development of human resources.

Mishchenko V. believes that the modern trend in the organization of personnel work at enterprises has become the use of an approach according to which, when selecting and hiring employees, personnel services are primarily focused on their experience, skills and opportunities for improving their professional level, and not on formal signs of education or qualifications (diploma, academic degree, license, certificate) [6, p.94]. The researcher actively uses the terms 'skill maps' and 'job architecture', which reflect the level of integration of skills into work and management processes by assigning them to groups of jobs, individual positions or performers [6, p.94]. Such practice allows for an individualized or personalized approach to developing employees' potential, forming their unique career trajectory and model of training and advanced training to achieve the level of competencies required for each next stage of movement on the way to occupying a higher position. Halinyak L., Spivak S., Marynyak B. prove that wartime brings radical changes to the management system at Ukrainian enterprises. Managers are expected to be highly mobile in making non-standard decisions and flexible in applying HR strategies. This requires the development of new effective methods for overcoming the personnel shortage. In particular, training, retraining of employees and the use of internal recruitment are relevant. It is necessary to implement a competent HR policy that would include an educational component [16, p.123].

A tangible problem for modern HR management is that company owners do not want to spend resources on developing or updating personnel policies and strategies, which significantly worsens their employer brand and becomes an obstacle to attracting talents to the workforce.

For most large enterprises, it has become a common practice to invest primarily in the training and development of existing employees who are well

aware of the specifics of the business and support the culture of the enterprise in a broad context [6, p.95]. At the same time, if we approach the issue of developing the potential of those people who are on the labour market in search of a vacant position, then the issues of organizing and financing such professionally oriented activities become the tasks of regional and state authorities. Therefore, it is advisable to integrate a set of measures aimed at maintaining and developing human capital in the regions of Ukraine into regional development strategies, and to foresee in local budgets the resources necessary for their financing.

It is worth agreeing with such scientists as Chorna L. O., Kudlayenko S. V., Chorna N. Yu., Kelmanovych O. that the transition to building management and business models, the basis of which is the development of business entities, provides opportunities for identifying, developing, uniting and properly rewarding the contribution of employees. The classical principles of HR management are being destroyed, and the emergence of new technologies has led to the improvement of HR management principles (for example, such as the principle of cooperation, transparency, openness, community, self-determination and others), that is, traditional approaches to HR management are giving way to more socially oriented and team-oriented ones due to the fact that employees of business entities are now inspired by their openness, autonomy, involvement and flexibility. Employers should recognize the value of individual contribution, ingenuity, initiative and enthusiasm, which are the driving force of the innovative strategy of business entities [14, p.7].

Therefore, we can summarize the list of problems of forming human resources in the regions of Ukraine in wartime conditions as follows:

- the movement of a significant part of the working population outside Ukraine or to rear regions;
- a decrease in the level of qualifications of the workforce available for recruitment on the domestic labour market;
- a reduction in the number of young people who in a few years will become the basis of the human resource for replenishing the staff of domestic enterprises;
- the low level of salaries that Ukrainian companies are ready to offer to specialists, stimulating their return to Ukraine or trying to keep them from dismissals and moving abroad;
- limited opportunities for non-state business structures to reserve key male employees;

- the reluctance of enterprises to attract employees on the terms of remote employment in the pursuit of total control over the performance of their duties;
- lack of trust between employees, their managers and top management of enterprises;
- lack of flexibility in policies for distributing working hours during the day, in particular, the unwillingness of management to take into account the interests and needs of employees when planning work schedules or vacations;
- problems with planning the working day for women with small children or other dependents;
- lack of opportunities to ensure the physical safety of workers at workplaces during air raids;
- low level of professional activity, initiative of young people who receive offers for internships in domestic companies;
- lack of effective cooperation between enterprises, institutions, business organizations and vocational and higher education institutions in the direction of updating educational programs for specific business needs and further employment of graduates of educational institutions (inability of enterprises to ensure that students undergo industrial practice or implement dual education using the material base of the business entity);
- lack of regional and state support for programs for the development of the population's human resources, their retraining and professional retraining to meet the personnel needs of the wartime economy.

The problem of forming human resources in the regions of Ukraine in wartime can be described as follows: the reluctance of highly qualified specialists to work for low salaries in conditions of constant threat to life; the passivity of personnel with low qualifications, no work experience or knowledge and skills that are irrelevant in the labour market to improve their professional level, lifelong learning, showing initiative and willingness to start a career trajectory from the lowest positions; the unwillingness of employers to offer flexible working conditions and competitive wages, the inability of the state to create opportunities for employment and professional growth of young specialists and male person through legislative changes.

23.3. The impact of digitalization and digital transformation risks on the human resources of enterprises and on their achievement of their strategic development goals

There is an opinion that modern digital technologies, such as artificial intelligence, data analytics, cloud technologies and process automation, are changing the way businesses operate. The introduction of these technologies into the field of human resources management allows enterprises to use resources more efficiently and optimize work processes. Therefore, the integration of modern digital technologies into human resources management policies and strategies is an important strategic direction of business development, which helps enterprises become more competitive, adaptive and attractive to potential employees [14, p.8], that is, to form a recognizable and desirable employer brand for employment in the regional and national labour markets.

Chernikova N.M. notes that digital transformations lead to changes in the composition and structure of personnel of enterprises of any industry. Modern innovative enterprises have a great need for programmers, business analysts, system administrators, testers, cybersecurity specialists, etc. [13, p.52].

Digitalization creates a new environment for doing business – another space for the emergence of risks and the need for personnel to counteract them while performing their duties. On the other hand, digital technologies become a means for employees of companies to commit malicious actions or cause accidental damage to their corporate resources, for example, due to the inability to correctly use digital resources and tools. This leads to the need to draw the attention of top management of enterprises to the management of personnel security, and in particular, the digital personnel security of the business. The concept of personnel security is defined by Nizhehorodtsev V., Petrenko L. as a set of conditions and factors that create security for the vital interests of participants in social and labour relations, contribute to the effective and harmonious development of human resources [7, p.159].

Thus, the impact of digitalization on the development of entrepreneurial activity carries a number of personnel threats. The main threat to the economic security of a company, which can be formed by the behaviour of employees in the digital economic space, is the leakage of confidential information about customers. Another feature in the field of personnel security is the danger of competitors luring the organization's leading

specialists. In addition to their professional competences, they carry confidential information about the activities of their former employer to the competitor. A significant threat to organizations is official misconduct committed by their own employees. Having access to the management of the organization's cash flows, they can abuse the employer's trust in various forms [7, p.162].

Chernikova N. M. summarized the problems of human resource provision of enterprises in the context of digital transformation, dividing them into two groups: problems for employers and problems for employees. The first group includes: a shortage of employees with a high level of digital literacy and the necessary digital competencies; outdated technologies and approaches to recruiting and selecting personnel for vacant positions, including a low level of use of digital recruiting; a lag in the amount of wages for domestic digital technology specialists by Ukrainian companies compared to the offers of foreign firms; demotivation of employees to master digital competencies, a low level of attractiveness and innovativeness of domestic enterprises, in particular, in the field of HR management, and an insufficient level of integration of digital technologies into the personnel management process; the inability of enterprises to guarantee the digital security of employees and the preservation of their personal data and the inconsistency of existing approaches in management with modern trends, the principles of socially oriented management and the goals of sustainable development. In the second group, the scientist combines such digital risks as the low level of digitalization of domestic enterprises and the incomplete formation of their digital ecosystems; the high cost of professional IT education in Ukraine, which is able to develop in an employee relevant competencies in the professional use of digital devices, technologies, information, etc.; the inconsistency of employees' competencies obtained in the process of obtaining professional higher education with the demands of modern business, including in the area of its digital development; the low level of protection of intellectual property, the creators of which are company employees, as well as the use by domestic business entities of imported software products, in particular, those that were created in the aggressor state, and therefore, can pose a significant threat to the cyber security of their users [13, p.54].

The largest digital risks for the personnel of modern enterprises are related to cybersecurity issues. Phishing, various attempts at unauthorized access to digital corporate and private accounts, through which fraudsters try

to obtain confidential information about the activities of the enterprise or the personal data of its top management, require the establishment of a digital information security system. There are also frequent cases when, after hacking, spam messages are sent from employees' corporate accounts to key clients, product consumers, partners, etc., in order to damage the business reputation of the enterprise or 'lure' financial resources on behalf of the company. The likelihood of successful implementation of such risks in practice increases if employees use 'weak' or 'monotonous' passwords when entering the enterprise's digital ecosystem or when creating corporate e-mail. It happens that employees inadvertently install malicious software on computers by downloading files or programs they need for work or for personal use. It is also important to note that digital risks to the economic security of a business entity increase if employees use personal electronic devices to perform their work tasks. In foreign countries, in order to counteract such risks, strict restrictions are imposed on the use of personal phones and laptops at workplaces or for performing official duties, and a system of fines and other forms of punishment is applied for violation of digital discipline. In Ukraine, such facts are difficult to track and record. In addition, domestic enterprises are not ready and do not have the opportunity to provide employees with official gadgets that they need for everyday work at their own expense. Therefore, permission to use personal devices (BYOD – Bring Your Own Device) is, although tacit and not approved in professional circles, still widespread in the Ukrainian business world, which creates a whole segment of opportunities in the digital space for the implementation of numerous digital threats, for example, such as "mixing" personal and work data, which can lead to accidental leakage of confidential information or its deletion when clearing the memory of a personal device.

Unobvious, but significant digital threats for both employees and their employers are information overload and emotional burnout due to the constant need for a company employee to be present in the digital space. It should be noted that 'information pressure' and the negative impact of 'digital noise' are felt more by middle-aged and older employees, while young people, who acquired professional competencies already in the digital era and under the influence of industry 4.0 trends, feel less fatigue from being in the digital environment. Therefore, the theory of ageism in HR management comes into play here. Information overload among employees occurs because the large amount of information they receive during the working day from various digital channels, such as social media groups, instant messengers,

website messages, email, corporate messages, etc., can reduce their concentration on urgent work issues, cause a sense of stress due to the likelihood of forgetting something, losing data, missing messages, and failing to complete an important assignment, and also lead to an increase in the number of errors when performing professional duties due to distraction from the sound signals of messages, calls, or the need to answer or react to them. Regarding the problem of fatigue and professional burnout, the need to constantly be in touch, to give feedback on digital messages, sometimes even after the end of the working day, leads to emotional exhaustion and a decrease in the employee's productivity, causes an increase in the level of his general dissatisfaction with work in the company and the emergence of a desire to terminate employment relations with the enterprise, the personnel policy of which focuses on the desire to constantly control the employee's availability to communicate in the digital environment.

A current opportunity to increase the level of digital literacy and increase the level of intellectual potential of the enterprise's human resources is the use of digital educational platforms. Having studied this issue in detail in his scientific research, Slatvinsky M. A. argues that digital educational platforms are important tools for developing the human resources of organizations, because they allow significantly increasing the efficiency of specialist training, reducing costs for it and providing a personalized approach to personnel development. However, their implementation requires overcoming a number of difficulties, such as technical problems, personnel resistance to change and the need to integrate into the overall strategy of the organization [11, p.218], which can also become a space for the emergence of additional digital risks for the information and economic security of the company.

Analysis of the digital support of the personnel component of the economic security system of the enterprise allowed scientists Nizhehorodtsev V. and Petrenko L. to highlight a number of the latest information and technological innovations aimed at achieving the global goals of the personnel service. Electronic petitions, the Unified State Portal of Administrative Services, the Cabinet of State Electronic Services, and other electronic services are powerful tools for the rather large-scale social transformations of today [7, p.169]. However, checking information about employees or candidates for positions does not give the company's management confidence that the employee has the appropriate level of digital literacy, understands digital risks, and is also ready to develop his own

intellectual potential in the direction of security-oriented use of digital capabilities to achieve the goals and interests of the business entity in a strategic perspective. Among the methods of personnel selection, employers often use tests to identify professional orientation, IQ test, psychological perception, erudition, intelligence, abilities and understanding, etc. [7, p.160]. And in the future, more and more attention will be paid to the HR management of modern business structures, especially those that intend to remain on the market for a long time and productively and conduct profitable financial and economic activities, to the search and development of the ability to use tools for diagnosing employees' competencies, talents and inclinations (including through tests, in particular psychological ones) in order to maintain a high level of personnel security of the enterprise and contribute to the growth of its human resources potential as the main intangible competitive advantage in the changing digital world.

References

1. Воронка, О. З. (2020). Формування тактики та стратегії забезпечення кадрової безпеки підприємства. Інноваційна економіка, No. 1-2, С. 99–10. <https://doi.org/10.37332/2309-1533.2020.1-2.15>
2. Дикань, О. В., Косінцева, П. Ю. (2023). Кадрове забезпечення процесу управління стратегічними змінами. Вісник економіки транспорту і промисловості, No. 81–82, С. 257–266. <https://doi.org/10.18664/btie.81-82.287171>
3. Дячков, Д. В., Богдан, М. О., Вовковінський, Ю. В. (2022). Сутність та роль управління кадровою безпекою підприємства в умовах цифровізації бізнес-середовища. Інфраструктура ринку, Вип. 69, С. 50–56. <https://doi.org/10.32782/infrastruct69-9>
4. Жуковська, В. М. (2019). Цифрові виклики кадрового забезпечення підприємства. Management and entrepreneurship in Ukraine: the stages of formation and problems of development, Vol. 1, No. 2, С. 10–17. <http://doi.org/10.23939/smeu2019.02.010>
5. Котелевець, Д. (2022). Тенденції кадрового забезпечення підприємств України в умовах цифрової економіки. Проблеми і перспективи економіки та управління, No. 2, С. 20–31. [http://doi.org/10.25140/2411-5215-2022-2\(30\)-20-31](http://doi.org/10.25140/2411-5215-2022-2(30)-20-31)

6. Міщенко, В. І. (2022). Забезпечення стійкості кадрового потенціалу підприємства в умовах цифровізації. Економічний простір, No. 182, С. 93–100. <https://doi.org/10.32782/2224-6282/182-14>

7. Ніжегородцев, В., Петренко, Л. (2022). Цифровий інструментарій кадрової складової системи економічної безпеки підприємства. Збірник наукових праць Державного податкового університету, No. 2, С. 155–172. <https://doi.org/10.33244/2617-5940.2.2022.155-172>

8. Павликівська, О. І., Галиняк, Л. О. (2022). Стратегічне забезпечення кадрового потенціалу підприємств. Галицький економічний вісник, Том 74, No. 1, С. 103–111. https://doi.org/10.33108/galicianvisnyk_tntu2022.0

9. Рекун, Г. П., Меденець, В. В. (2020). Механізм управління стратегічними розривами кадрового забезпечення розвитку регіону. Економічний форум, No. 3, С. 30–39. Available at: http://nbuv.gov.ua/UJRN/ecfor_2020_3_7

10. Рудзін, Д. С. (2024). Розвиток кадрового потенціалу публічного управління в умовах цифровізації суспільства. Державне управління: удосконалення та розвиток, No. 5. Available at: http://nbuv.gov.ua/UJRN/Duur_2024_5_23

11. Слатвінський, М. А. (2024). Цифрові освітні платформи: нові можливості у розвитку кадрового потенціалу організацій. Економічний простір, No. 196, С. 217–224. <https://doi.org/10.30838/EP.196.217-224>

12. Токмакова, І. В., Корінь, М. В., Полозов, А. Є., Авагімова, В. А. (2024). Кадрове забезпечення інноваційно-цифрової модернізації підприємств. Вісник економіки транспорту і промисловості, No. 86, С. 276–286. <https://doi.org/10.18664/btie.86.317290>

13. Чернікова, Н. М. (2020). Проблеми кадрового забезпечення підприємств в умовах цифрових перетворень. Вісник Хмельницького національного університету. Економічні науки, No. 4(2), С. 52–55. [https://doi.org/10.31891/2307-5740-2020-284-4\(2\)-9](https://doi.org/10.31891/2307-5740-2020-284-4(2)-9)

14. Чорна, Л. О., Кудласенко, С. В., Чорна, Н. Ю., Келманович, О. (2024). Кадрове управління та його техніко-технологічне забезпечення як складова оперативного та стратегічного менеджменту. Агросвіт, No. 10, С. 4–11. <https://doi.org/10.32702/2306-6792.2024.10.4>

15. Приходько, Л. С., Білоус, С. П. (2024). Управління комунікаційною політикою суб'єкта господарювання для потреби забезпечення його кадрової безпеки та цілей стратегічного розвитку. Міжнародний науковий журнал "Інтернаука", No. 10, С. 18–24. <https://doi.org/10.25313/2520-2057-2024-10-10395>

16. Галиняк, Л., Співак, С., Мариняк, Б. (2024). Розроблення стратегії кадрового забезпечення як елемента освітнього потенціалу підприємства. Галицький економічний вісник, Том 88, № 3. С. 122–129. https://doi.org/10.33108/galicianvisnyk_tntu2024.03.122

Chapter 24
***Digital management in ensuring the economic security of
organizations under the dominance of Big Tech***
(V. Voloboiev)

The European economy is undergoing a profound digital transformation that is reshaping market structures, the logic of competition, and approaches to management. At the same time, the key components of the digital environment (search, cloud computing, social networks, mobile ecosystems) remain under the total control of a limited number of global corporations known as Big Tech. As a result, conditions are emerging in which European companies actively implement digital technologies but are forced to operate in an environment where the rules are defined by actors external to the EU.

This situation generates a number of challenges to economic security. Limited competition weakens innovation dynamics, creates risks of price dictate, and complicates market entry for new participants. An additional threat is the opacity of algorithms and the lock-in effect, which restrict strategic business autonomy and reduce capital mobility. Under these conditions, digital management acquires particular importance as a system of managerial decisions capable of combining the use of digital tools with the maintenance of business competitiveness.

The purpose of this chapter is to analyze the impact of Big Tech on the economic security of organizations in the EU, to identify the main risks of monopolization of the digital space, and to outline areas of digital management that can ensure a balance between leveraging the opportunities of digitalization and protection against external threats.

24.1. The impact of Big Tech on the economic security of organizations

In the modern economy, the digital space is increasingly concentrated within the sphere of influence of a limited number of transnational corporations, collectively known as Big Tech. These include Alphabet Inc. (the parent company of Google LLC), Apple Inc., Microsoft Corporation, Amazon.com Inc., and Meta Platforms Inc. (the parent company of Facebook, Instagram, WhatsApp, and other services). These companies form distinctive ‘digital ecosystems’ that integrate search services, advertising platforms, communication channels, mobile operating systems, and cloud infrastructure. Such market concentration (Fig. 24.1) creates not only new tools for business development but also generates a number of threats to its economic security.

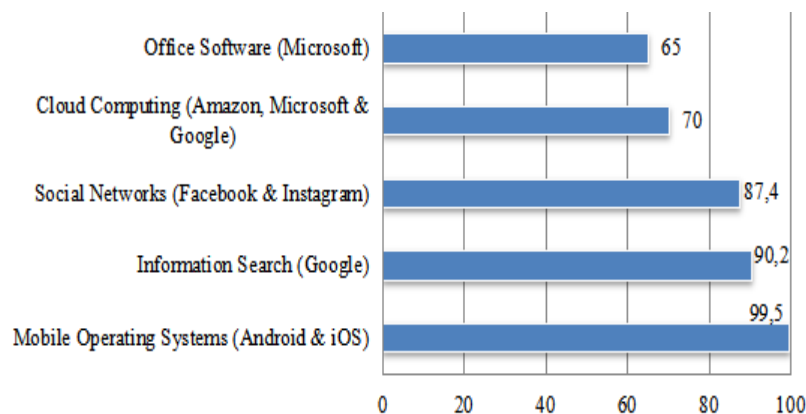


Fig. 24.1. Share of dominant players in the EU market across different segments of the digital economy, %

Compiled by the author based on: [1,2,3,4,5]

In the field of information search, an unprecedented level of dominance is observed: Google’s share in the European segment exceeds 90% [1], which effectively deprives businesses of alternative channels for ensuring their presence in the online search environment. This dependence makes any changes in algorithms or advertising policies decisive for thousands of companies, regardless of their size or sector of activity.

Similar trends are observed in the field of social communications. Meta platforms (Facebook, Instagram, and WhatsApp) reach more than 87% of social media users in Europe [2]. This means that digital marketing and

customer interaction are largely determined by a single corporation that controls the rules of access.

The mobile segment is characterized by a duopoly of Apple (iOS) and Google (Android): in the European market, Android accounts for about two thirds, while iOS covers nearly one third of consumers [3]. Together, these companies form closed environments in which control is exercised not only through operating systems but also through app stores that define the distribution channels for digital products.

Another critically important area is cloud computing. Here, leading positions are held by Amazon, Microsoft, and Google, which together control about 70% of the European market [4]. For organizations, this creates a dual risk: 1) high dependence on infrastructure located outside EU jurisdiction; 2) vulnerability to changes in pricing and technical access conditions.

It is also worth noting the role of Microsoft: the use of Office 365 accounts for about 65% in the EU corporate sector [5], which indicates significant dominance in the field of document management and business communications.

Despite the undeniable advantages associated with the development of digital infrastructure and the diffusion of innovative services, Big Tech dominance is accompanied by a number of systemic risks with long-term consequences. The concentration of power in key segments of the digital economy gradually alters the logic of competition. This leads to the emergence of ‘digital barriers’ that complicate market entry for new participants, narrow the range of available technological alternatives, and weaken the ability of businesses to maintain strategic autonomy. For states, such a situation implies not only economic but also regulatory dependence on global platforms whose decisions often lie beyond national jurisdiction and define the rules of the game in strategically important sectors. Ultimately, the negative effects of Big Tech dominance should be viewed not merely through the lens of classical market distortions, but as a comprehensive challenge to economic security. This challenge manifests itself in the slowing of innovation processes, distortion of pricing policies, the emergence of barriers to market access, reduced capital mobility, and increased dependence on closed technological ecosystems.

The dominance of Big Tech weakens incentives for technological renewal. Instead of developing competing products, leading corporations often integrate potential competitors into their own platforms. According to available estimates, companies from the ‘Big Five’ acquire, on average, one

startup every eleven days, resulting in more than 190 acquisitions over just six years [6]. Examples of such deals include Apple's acquisition of the French company Datakalab in 2023 and Meta's acquisition of the Swedish startup Mapillary in 2020. Such practices pose a systemic threat to the European innovation environment, as companies with unique technologies lose the opportunity for independent development, while their solutions are absorbed into the global ecosystems of Big Tech, narrowing the space for the emergence of independent players.

The monopolistic position allows corporations to shape pricing policies outside market mechanisms. This is particularly evident in cases of the lock-in effect, when organizations become "locked" into the services of a single provider and lack the ability to quickly switch to alternatives [7]. In the cloud segment, Microsoft has established licensing conditions for Windows Server and SQL Server that make the use of these products in competing clouds significantly more expensive than on Azure. According to estimates by CISPE (Cloud Infrastructure Services Providers in Europe), this creates more than EUR 1 billion in additional annual costs for EU businesses and effectively restricts competition. At the same time, Apple maintains a commission of up to 30% in the App Store, shaping prices for developers and consumers, which has become the subject of antitrust proceedings by the European Commission. Google, through its Shopping service, gave priority to its own listings in search results, and in 2024 the Court of Justice of the EU confirmed the EUR 2.4 billion fine imposed back in 2017. Within its Marketplace, Amazon gave preference to its own products, as confirmed by an investigation of the European Commission. All these practices directly affect cost structures and pricing: companies are forced to adapt to the conditions imposed by large corporations, while market pricing is determined by the policies of a few global players, undermining the financial autonomy of businesses and creating long-term risks to economic security.

The influence of Big Tech also extends to companies' ability to enter digital markets. In 2023, the European Commission launched an antitrust investigation into the integration of the Teams service into the Microsoft 365 suite, which created an advantage for the corporation's own product and hindered the entry of alternative services, such as Slack, into the corporate segment. Such mechanisms demonstrate how, due to monopolistic positions, new players face disproportionately high barriers to accessing users.

In the field of digital advertising, similar restrictions have been identified in Meta's activities. In 2023, the European Commission initiated

an investigation into the ‘pay-or-consent’ model, under which access to Facebook and Instagram services was provided only on the condition of personal data collection or payment. This approach was assessed as a violation of the provisions of the Digital Markets Act, as it deprived businesses of the ability to interact with customers under privacy-preserving conditions.

The concentration of digital power also affects investment decision-making practices, in particular by channeling funding toward projects capable of integrating into already established platforms. Although this does not determine the overall volume of venture financing in the EU, it creates an additional imbalance in its distribution. Combined with institutional and market factors, this explains why the level of venture capital investment in the EU is about 0.3% of GDP compared to more than 0.9% in the United States [8].

An additional factor affecting capital mobility is the phenomenon of kill zones, which emerges after startups are acquired by large corporations. In such cases, venture investors become more cautious about financing similar directions, which reduces innovation dynamics and increases dependence on dominant players. As shown by the research of Gugler et al., these effects are not limited to the short term: in a number of segments they have a more persistent impact, creating structural imbalances in venture financing and weakening the development of independent innovation ecosystems in the EU [9].

The economic effects of monopolization of digital markets extend beyond individual companies and have a macro-level dimension for public finances and the revenue structure of the EU.

First, there is a ‘drain’ of financial resources through tax optimization by transnational platforms: researchers’ estimates indicate significant shortfalls in corporate tax revenues [10], which the new rules on global minimum taxation are intended to correct only partially.

Second, a permanent imbalance is formed for small and medium-sized enterprises: SMEs interact with platforms from extremely weak positions, with a lack of information transparency and a high degree of dependence on integrated services (advertising, logistics, analytics). A study by the European Parliament found that SMEs in digital advertising often lack sufficient data and ‘leverage’ to ensure fair representation, which directly increases their customer acquisition costs and complicates planning [11].

Third, profits and value added are increasingly concentrated within a small group of ‘superstar’ digital companies. This intensifies the profitability gap between large platforms and the rest of market participants. Analysis by the European Commission shows a growing share of such companies in the total profits of the EU corporate sector, which is consistent with international observations on the redistribution of rents in favor of the upper segment of firms [12].

Thus, the dominance of Big Tech in the EU is systemic in nature: it manifests itself in the monopolization of key segments of the digital economy, the formation of business dependence on global platforms, the weakening of SMEs’ positions, and the concentration of profits within a small group of corporations. Such trends undermine the economic security of organizations, reduce their autonomy, and create long-term risks for the competitive environment. In this context, the task arises of developing and implementing digital management tools capable of minimizing the negative effects of monopolization and ensuring business economic security under conditions of digital dependence.

24.2. Instruments of digital management for ensuring the economic security of organizations

Under current conditions of Big Tech dominance, European companies face a number of systemic problems that directly affect their digital autonomy and economic security. The main consequences of this situation include the loss of control over user data, constraints on strategic decision-making, high dependence on external platforms for marketing and analytics, as well as increased risks of cyberattacks and information leakage.

For each identified consequence of Big Tech dominance, a corresponding digital management instrument has been defined, the application of which is aimed at strengthening the economic security of EU business organizations. Let us consider each of the proposed instruments in more detail.

1. Loss of control over user data and analytics.

Dependence on Big Tech in the field of analytics manifests itself primarily at the strategic level. By transferring data collection and processing to external platforms, organizations effectively delegate their ability to independently form an understanding of their own customers. This reduces

strategic autonomy, as decisions are made based on interpretations generated by Big Tech algorithms rather than on internal analytics.

An adequate response to this problem lies not only in the choice of alternative tools, but above all in the development of a corporate data governance policy. This involves the formalization of internal rules for data collection, storage, and analysis, the establishment of dedicated responsibility centers, and the integration of analytics into the strategic planning system of organizations. In a number of European companies, internal analytics systems have already been implemented, allowing full control over data processing and compliance with regulatory requirements. However, the practical implementation of these measures is characterized by certain limitations that must be taken into account. First, management often faces a lack of sufficient data for comprehensive analytics, which complicates the development of forecasting models. Second, the creation of internal systems requires not so much technical investment as the development of new managerial competencies. To overcome these limitations, it is advisable to introduce sectoral forms of cooperation, whereby several companies create shared data pools to mutually strengthen analytics. In the long term, this may form the basis for the development of European data alliances that would allow businesses to reduce their dependence on global corporations.

2. Risk of data leakage and digital security breaches.

A critical manifestation of dependence on Big Tech is the vulnerability of businesses to confidentiality breaches and data leaks. The use of third-party platforms for data storage and processing means that companies effectively transfer control over customers' private data to external corporations. In the event of data breaches or non-compliance with GDPR requirements, it is the business that remains responsible to regulators.

Digital management instruments in this context should focus on regulatory compliance and internal control. This involves the development of cybersecurity and risk management policies that include regulation of data access, operational audits, regular inspections, and staff training. European practice, particularly in the banking sector and telecommunications, demonstrates the effectiveness of this approach: multi-level access systems, real-time transaction monitoring, and internal compliance checks against security standards.

For companies that are unable to maintain large in-house teams, an alternative is the use of outsourcing solutions in the format of 'security-as-a-service' (SECaaS). This makes it possible to integrate protective tools without

significant capital expenditures while ensuring compliance with regulatory requirements. A promising direction is also the implementation of data governance systems that combine data management and security policies, creating a transparent and controlled foundation for working with information.

3. Vulnerability to cyberattacks through third-party services.

Another dimension of dependence on Big Tech is related to the fact that companies entrust the security of their data to external infrastructures that remain outside their direct control. This creates a dual risk: on the one hand, potential cyberattacks on the providers themselves, and on the other, a loss of autonomy, as decisions on incident response are made not by the company but by an external corporation. Under such conditions, businesses are transformed from users of technology into hostages of third-party security strategies.

Digital management tools in response to this challenge should be aimed at preserving autonomy and diversifying sources of protection. First and foremost, this involves the establishment of internal or partner-based monitoring and incident response centers that enable control over incidents independently of Big Tech cloud solutions. For small and medium-sized enterprises, the use of previously mentioned SECaaS solutions from independent providers operating outside the ecosystems of global corporations is appropriate. This creates competition, allows risks to be distributed, and helps avoid monopolized security arrangements.

An important set of tools also includes mechanisms to ensure data portability and the development of exit strategies. These instruments guarantee the continuity of managerial processes even in the event of migration to another service, facilitate transitions, and provide companies with the ability to leave Big Tech ecosystems without losing control over their operations.

4. Limited autonomy in decision-making due to external services.

Dependence on Big Tech brings to the forefront the issue of companies' independence in strategic management. Many decisions related to marketing, demand forecasting, or pricing are made under the influence of algorithms developed by Google, Microsoft, Apple, and others. These models operate as 'black boxes' and generate recommendations that businesses often accept without the possibility of critical verification. Today, individual cases can be found where large retailers develop internal forecasting systems, for example by creating their own machine-learning models for inventory management.

However, such examples remain isolated and do not constitute a systemic alternative to Big Tech.

For this reason, it is appropriate to propose a new managerial direction within digital management – the development of internal AI-driven decision-making systems. This refers not only to local forecasting models, but to the construction of integrated corporate systems that combine data from internal processes (CRM, ERP) and enable strategic decisions to be made without full dependence on external services. Such a system may include: 1) corporate data platforms as a source of ‘raw’ data; 2) proprietary algorithms for forecasting demand or customer behavior; 3) decision-support modules for managerial scenarios (what-if analysis, scenario modeling).

It should be noted that the key constraints on implementing this approach are the high cost of system development and the lack of high-quality data. However, these barriers can be mitigated through the sectoral cooperation mechanisms described above. In the financial sector, such approaches are being tested in the form of banking consortia that create joint AI systems for risk assessment. In the long term, similar models may be scalable to other industries as well.

5. Dependence on Big Tech advertising platforms.

One of the most obvious and at the same time strategically vulnerable forms of business dependence on Big Tech is reliance on their advertising ecosystems. For many companies, Google Ads or Meta Ads become the primary, and sometimes the only, channel of communication with the target audience. This creates situations in which any changes in platform policies or algorithms directly affect the financial results of businesses, reducing controllability and predictability.

A practical way out of this dependence is demonstrated by the retail sector, where retail media networks (RMN) are actively developing – proprietary advertising ecosystems of retail chains. They allow brands to place advertising directly on retailers’ digital assets (websites, mobile applications, loyalty platforms) and even in physical stores. This format relies on the use of first-party customer data collected by retailers through transactions, which enables more precise targeting and more accurate measurement of advertising effectiveness.

At present, RMNs have become one of the fastest-growing channels of digital advertising. For retailers themselves, this means a new source of revenue and strategic autonomy, as they not only control the advertising infrastructure but also retain a critical channel of access to consumers without

the intermediation of Big Tech. It should be noted that in retail the feasibility of such cases is explained by the presence of two key factors: 1) significant volumes of first-party data generated through daily transactions and loyalty programs; 2) retailers possess extensive channels of direct interaction with customers, which makes it possible to integrate advertising tools into their own digital infrastructure and control the entire cycle from ad exposure to purchase. These characteristics make the sector the most suitable for the formation of corporate media platforms.

At the same time, the direct transfer of retail-specific use cases to other industries is not feasible. In particular, in B2B sectors (industry, energy, construction) there are no large-scale data sets or broad communication channels with end customers, which makes the creation of full-fledged RMNs impossible. In sectors subject to increased regulatory control (finance, healthcare), barriers related to the use of personal data, GDPR restrictions, and sector-specific legislation also constrain the development of advertising ecosystems based on first-party data.

For such industries, the use of alternative approaches is appropriate. First, this includes the creation of industry consortia that allow the pooling of data from several companies to form joint communication platforms. Second, an important direction is the development of proprietary digital customer interaction services (portals, applications, loyalty systems), which can reduce dependence on external advertising channels even without the scale typical of retail. Third, the use of open-source and custom marketing automation systems is promising, as it allows organizations to retain control over data within the company and avoid dependence on Big Tech as SaaS providers.

6. Limitations on the development of digital sovereignty.

Dependence on the infrastructural services of Big Tech is increasingly emerging as a strategic challenge for European enterprises. Organizations that operate entirely within the ecosystems of Google, Amazon, or Microsoft are effectively deprived of the ability to shape their own digital standards and architectures, since key business processes are carried out according to the rules set by external providers. This implies not only technical but also managerial vulnerability: companies delegate control over data processing, digital communication channels, and conditions of access to customers to global corporations, which significantly limits opportunities for developing their own digital sovereignty.

In response to this challenge, intergovernmental initiatives are being implemented in the EU, in particular the GAIA-X project, aimed at creating

an open and interoperable cloud infrastructure for business and the public sector. Its objective is the formation of data spaces for strategic sectors such as healthcare, energy, mobility, and finance, which would allow enterprises to retain control over their own information resources and avoid critical dependence on American technology giants.

At the corporate level, attempts to regain control over critical functions of digital management are reflected in the development of internal platforms for data storage and processing, customer communications, and marketing management. For large EU corporations, this practice has already become a new standard: companies invest in their own data centers, CRM systems, and mobile applications, which makes it possible to gradually reduce the role of external providers in strategic processes. An example is Telefónica Tech, which develops services in the areas of cloud computing, edge solutions, and artificial intelligence in line with the principles of European digital sovereignty.

At the same time, for small and medium-sized enterprises such a strategy is often unattainable due to financial and technological barriers. In these cases, it is more appropriate to speak not about building full-fledged corporate data ecosystems, but about adaptive models of partial sovereignty: the use of open-source solutions for CRM and marketing automation, as well as the gradual integration into European initiatives such as GAIA-X.

In general, the development of corporate digital platforms cannot completely eliminate dependence on Big Tech; however, it functions as a tool for the gradual acquisition of autonomy. For large companies, this has already become a common practice, whereas for smaller organizations the strategic value lies in the formation of hybrid solutions that reduce risks and lay the foundations for their own digital sovereignty.

24.3. Institutional influence on the transformation of digital management of organizations in countering the dominance of Big Tech

The contemporary dynamics of digital economy development are shaped not only by technological innovations but also by profound institutional changes that define the conditions under which organizations operate in the global environment. In a situation where Big Tech controls critical segments of digital infrastructure and information flows, the institutional environment plays a key role in ensuring the autonomy of digital governance. This influence manifests itself in the transformation of digital

management, which gradually moves beyond the instrumental use of platforms and becomes a strategic resource for countering the excessive concentration of power in the digital space.

The formation of the institutional environment in the EU is directly aimed at limiting the market power of global corporations and creating conditions for the more autonomous development of national and corporate digital strategies. The adoption of the General Data Protection Regulation became the starting point of these changes, as it established a fundamentally new model of data governance. In the context of digital management, the implementation of GDPR led to three core transformations: 1) a transition to a new data governance model based on data minimization, transparency of processing, and the enforcement of the right to erasure; 2) the institutionalization of mechanisms for obtaining and recording user consent within digital systems; 3) the formation of organizational data protection practices through the introduction of the role of the Data Protection Officer, regular risk assessments, and the integration of ‘privacy by design’ principles (proactive prevention, data minimization, integration into the product, balance between value and protection, lifecycle security, transparent processes, and user control over data) into the digital product development process. In a number of European corporations, including Deutsche Telekom and Siemens, this resulted in the establishment of specialized data compliance units integrated into the digital management structure. Their activities include monitoring algorithmic transparency, controlling user consent processes, and incorporating data protection indicators into the KPIs of digital project managers.

In the institutional dimension, a number of gaps remain that reduce the effectiveness of countering the market power of global digital corporations and require additional regulation.

First, the issue of cross-border data transfers remains unresolved. Following the invalidation of previous agreements, the legal framework remains fragmented, which creates vulnerabilities for the digital management of organizations and calls into question the EU’s digital sovereignty. Similar challenges are outlined in a study by the European Data Protection Board, which demonstrates the limited effectiveness of GDPR enforcement tools with regard to companies located outside the EEA but whose activities extend to EU citizens [13].

Second, there is an observable economic asymmetry whereby small and medium-sized enterprises bear disproportionately high costs in complying

with GDPR requirements. This is confirmed by empirical studies showing that the regulatory burden for SMEs is significantly heavier compared to large corporations [14]. Similar conclusions have been reached in the context of technology startups in Catalonia, where it is emphasized that GDPR creates substantial financial and human resource challenges for small firms [15].

Third, there is the problem of heterogeneity in the application of the regulation at the national level. Differences in the practices of supervisory authorities reduce the overall effectiveness of oversight of Big Tech. This is supported by a systematic literature review pointing to fragmentation in GDPR implementation and uneven enforcement across EU member states [16].

The further development of regulatory policy in the form of the Digital Markets Act and the Digital Services Act has created legal preconditions for limiting the influence of gatekeepers (large online platforms that exert significant influence on the internal market and act as intermediaries between businesses and users). Requirements concerning algorithmic transparency, restrictions on abusive market practices, and strengthened liability for content have compelled companies to reconsider their digital presence strategies. As a result, digital management practices have begun to transform toward channel diversification, the development of multi-layered communication models, and investment in proprietary digital solutions. The introduced regulation has also acted as a catalyst for initiatives such as GAIA-X, which illustrate a shift from the non-alternative use of Big Tech cloud services toward the integration of European infrastructure. In the field of digital management, this entails revising data governance policies and adapting corporate processes to European standards.

Improving the institutional environment in the field of digital regulation requires a comprehensive set of measures aimed at addressing identified structural imbalances and strengthening the effectiveness of data protection rules. Above all, this involves establishing a stable mechanism for cross-border data transfers based on transparent international agreements and the development of European data centers capable of ensuring autonomous management of information flows. Equally important is the creation of adaptive compliance procedures for small and medium-sized enterprises that would reduce the regulatory burden, in particular through standardized templates, advisory services, and financial support mechanisms. In addition, harmonization of enforcement practices within the EU is required by strengthening the coordinating role of the European Data Protection Board

and introducing unified approaches to the interpretation and monitoring of compliance with regulatory norms.

Further improvement of the institutional environment should focus on the practical specification of the requirements of the Digital Markets Act and the Digital Services Act, in particular through the development of unified standards for algorithmic transparency, clear criteria for identifying and preventing abuses of market power, and mechanisms for effective content monitoring without imposing excessive administrative burdens on businesses. Equally important is the establishment of European systems for algorithm auditing and independent centers of expertise capable of ensuring compliance with the new rules in a manner that reduces dependence on Big Tech. For organizational digital management, these changes should be implemented through increased transparency of business processes, the need for institutional risk monitoring, and the integration of algorithm audits into the system of strategic management.

Taken together, these measures will contribute to strengthening digital sovereignty, reducing dependence on global technology corporations, and enhancing the effectiveness of digital management at the corporate level.

The issue of digital sovereignty in the European Union has gained particular relevance amid the growing dependence of businesses on the infrastructure of global digital corporations. In academic discourse, this phenomenon is viewed as a multidimensional category that combines institutional, technological, and regulatory dimensions. Thus, Santaniello [17] interprets digital sovereignty as a set of attributes, including control over key technologies, autonomy in decision-making, and a reduction of dependence on external actors. Roberts [18] proposes a normative approach, emphasizing that digital sovereignty is based not only on technical control but also on the legitimate right to define the conditions under which the digital environment operates. By contrast, Baldoni and Di Luna [19] focus on the technological dimension, defining digital sovereignty as the ability to ensure continuous access to reliable infrastructural capacities, without which economic security cannot be guaranteed. The political dimension of the concept is explored by Hulkó et al. [20], who show that EU digital sovereignty is becoming a tool for countering external influence and for shaping an autonomous European digital model.

Thus, in scholarly approaches, digital sovereignty is considered a strategic prerequisite for the development of the EU's digital economy. Its impact is directly felt by organizations, as the implementation of policies and

strategic programs changes the very logic of digital management – from an orientation toward adapting to the rules of Big Tech to the formation of managerial decisions that increase the degree of business autonomy. At the practical level, this is reflected in support for ‘national champions’ such as OVHcloud (cloud infrastructure services as an alternative to Amazon Web Services or Microsoft Azure), Deutsche Telekom (telecommunications and cloud platforms, including Open Telekom Cloud as a European alternative to global providers), and SAP (corporate software solutions for business process management that serve as substitutes for Oracle or Microsoft Dynamics products). Owing to EU institutional support, these companies are able to offer businesses alternative services. For digital management, this translates into the emergence of a strategic option to choose local solutions.

The development of national Computer Emergency Response Teams (CERTs) has a direct impact on managerial practices in the digital domain. Digital management can no longer be limited to marketing and communications and increasingly integrates functions related to risk management and cyber resilience. This shifts the substance of digital activity: companies establish internal monitoring systems, and incident management becomes part of everyday operational activity. In the EU, this direction already has a solid foundation – most notably, the NIS2 Directive and the preparation of the Cyber Resilience Act have formalized requirements for mandatory incident reporting and minimum-security standards.

Equally important is the role of public-private partnerships, which at the EU level are institutionalized through programs such as the European Alliance for Industrial Data, Edge and Cloud and initiatives within the European Data Strategy. These frameworks shape political and legal conditions for the joint governance of data and infrastructure, setting standards of openness, transparency, and interoperability (the ability of different digital systems, platforms, and organizational infrastructures to exchange data freely and function together effectively). For the digital management environment, this translates into the need to account for external regulatory requirements when designing corporate processes, including the integration of data exchange standards and the development of internal interoperability procedures.

Further development of institutional mechanisms of digital regulation will not only constrain the market power of Big Tech within the European space but will also gradually transform the very logic of digital management in organizations. Whereas at early stages digital management was primarily

understood as a supporting tool for addressing current operational tasks, under the influence of new regulatory frameworks it increasingly acquires a strategic character. Organizations are compelled to integrate into digital management not only issues of customer experience or market presence, but also aspects of data control, algorithmic transparency, localization of information flows, and compliance with cyber resilience requirements. This shift signifies the transition of digital management from a supporting role to an architectural function that defines the possibilities for autonomous development.

Managerial logic must also change from an orientation toward rapid efficiency to the prioritization of long-term resilience. Key metrics increasingly focus on data control, the ability to operate across different regulatory environments, the stability of digital infrastructure, and the transparency of algorithmic processes.

At the same time, the transformation perspective reveals a number of challenges. The most acute among them is a skills shortage: organizations lack managers capable of combining an understanding of market strategy with competencies in regulatory frameworks, cyber resilience, and data governance. This necessitates a revision of educational programmes, the development of new professional profiles, and the reskilling of existing management personnel.

In the longer term, organizational digital management will evolve into a multidimensional system that integrates strategic planning, data control, risk management, the development of multichannel interaction models, and the resilience of digital infrastructure. Its key distinction from earlier stages will lie not in the use of individual tools or platforms, but in the ability to design an architecture of digital autonomy in which Big Tech loses its monopolistic position, thereby opening opportunities for diversification and enhancing the level of economic security of EU organizations.

Thus, the materials of the present study demonstrate that the influence of Big Tech on the economic security of organizations in the European Union is systemic in nature. The concentration of power in the areas of search, communications, mobile ecosystems, and cloud services creates persistent dependencies that constrain innovation potential, complicate market entry for new participants, and affect enterprise development. This confirms that the strategic risks of digital monopolization should be viewed not merely as isolated manifestations of distorted competition, but as a multidimensional threat to business economic security.

In this context, digital management can be regarded as one of the effective means capable of ensuring a balance between leveraging digital infrastructure opportunities and protecting organizations from excessive dependence. The introduction of data governance policies, the development of internal analytics systems, the advancement of cyber resilience mechanisms, the diversification of communication channels, and the creation of conditions for data portability gradually transform digital management into an instrument for preserving organizational autonomy. It is precisely the integration of these instruments into the system of strategic management that enables the mitigation of the negative effects of Big Tech dominance and the enhancement of enterprises' economic security.

Further transformation of digital management in the EU is possible only under conditions of improving the institutional environment, which should not only entrench regulatory norms but also create conditions for their practical integration into corporate strategies. This involves the establishment of a stable mechanism for cross-border data transfers, the harmonization of enforcement practices within the EU, the introduction of European standards of algorithmic transparency, and the development of independent audit centers. For digital management, this will imply an expanded toolkit for data control, increased compliance effectiveness, and the ability to implement long-term models of autonomous business development. At the same time, the expected outcome of these changes is, on the one hand, a reduction in the degree of organizational dependence on Big Tech and, on the other hand, the formation of greater autonomy in those segments where a complete withdrawal from the services of large corporations is not feasible.

References

1. Search Engine Market Share Europe. *StatCounter*. Available at: <https://gs.statcounter.com/search-engine-market-share/all/europe>
2. Social Media Stats Europe. *StatCounter*. Available at: <https://gs.statcounter.com/social-media-stats/all/europe>
3. Mobile Operating System Market Share Europe. *StatCounter*. Available at: <https://gs.statcounter.com/os-market-share/mobile/europe>
4. European Cloud Providers' Local Market Share Now Holds Steady at 15%. *SRG Research*. Available at: <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>

5. Microsoft Office 365 vs. Google G Suite (EMEA). *ChannelE2E*. Available at: <https://www.channele2e.com/news/microsoft-office-365-vs-google-g-suite-emea>

6. Big Tech Acquires a New Company Every 11 Days. *SOMO*. Available at: <https://www.somo.nl/big-tech-acquires-a-new-company-every-11-days>

7. Vendor Lock-In and Interoperability: Importance of Interoperability among Cloud Services. *ResearchGate*. Available at: https://www.researchgate.net/publication/383855750_Vendor_Lock-In_and_Interoperability_Importance_of_interoperability_among_cloud_services

8. Arnold, N. G., Claveres, G., Fri, J. (2024). Stepping Up Venture Capital to Finance Innovation in Europe. *International Monetary Fund*. Available at: <https://www.imf.org/en/Publications/WP/Issues/2024/07/10/Stepping-Up-Venture-Capital-to-Finance-Innovation-in-Europe-551411>

9. Gugler, K., Szücs, F., Wohak, U. (2025). Start-up acquisitions, venture capital and innovation: A comparative study of Google, Apple, Facebook, Amazon and Microsoft. *International Journal of Industrial Organization*. Vol. 99. <https://doi.org/10.1016/j.ijindorg.2025.103148>

10. Global Tax Evasion Report 2024. *EU Tax Observatory*. Available at: https://www.taxobservatory.eu/www-site/uploads/2023/10/global_tax_evasion_report_24.pdf

11. Online advertising: the impact of targeted advertising on advertisers, market access and consumer choice. *European Parliament*. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662913/IPOL_STU%282021%29662913_EN.pdf

12. Bustelo, J. L. G., Pérez, A. M., Meruvia Torrez, H. (2025). The Determinants of the Concentration of Superstar Firms: Cluster Analysis and Its Relationship with Economic Development and Artificial Intelligence. *Economies*. Vol. 13, No. 2, Art. 52. <https://doi.org/10.3390/economies13020052>

13. Finance Threat Landscape 2024. *ENISA*. Available at: https://www.enisa.europa.eu/sites/default/files/2025-02/Finance%20TL%202024_Final.pdf

14. Blind, K., Niebel, C., Rammer, C. (2024). The impact of the EU General Data Protection Regulation on product innovation. *Industry and*

Innovation. Vol. 31, No. 3, pp. 311–351.
<https://doi.org/10.1080/13662716.2023.2271858>

15. Smirnova, Y., Travieso-Morales, V. (2025). Tech startups and General Data Protection Regulation: an empirical exploration of compliance challenges. *Journal of Small Business & Enterprise Development*. Vol. 32, No. 8, pp. 54–82. <https://doi.org/10.1108/JSBED-09-2024-0495>

16. Smirnova, Y., Travieso-Morales, V. (2024). Understanding challenges of GDPR implementation in business enterprises: a systematic literature review. *International Journal of Law and Management*. Vol. 66, No. 3, pp. 326–344. <https://doi.org/10.1108/IJLMA-08-2023-0170>

17. Santaniello, M. (2025). Attributes of Digital Sovereignty: A Conceptual Framework. *Geopolitics*, pp. 1–22.
<https://doi.org/10.1080/14650045.2025.2521548>

18. Roberts, H. (2024). Digital sovereignty and artificial intelligence: a normative approach. *Ethics and Information Technology*. Vol. 26, Art. 70.
<https://doi.org/10.1007/s10676-024-09810-5>

19. Baldoni, R., Luna, G. D. (2025). Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities. *IEEE Security & Privacy*. Vol. 23, No. 1, pp. 91–96.
<https://doi.org/10.1109/MSEC.2024.3500192>

20. Hulkó, G., Kálmán, J., Lapsánszky, A. (2025). The politics of digital sovereignty and the European Union's legislation: navigating crises. *Frontiers in Political Science*. Vol. 7.
<https://doi.org/10.3389/fpos.2025.1548562>

Chapter 25

Environmental and digital transformation as instruments for strengthening global economic security: strategic objectives and outcomes of the European Union

(I. Taranenko, A. Mostova, H. Zhykhareva-Tolstik)

Environmental (green) and digital transformations are defined as strategic instruments for strengthening global economic security, and this fully applies to the European Union. The European Green Deal aims to reduce energy dependence, minimise climate-related risks, and diversify resource supplies, thereby directly decreasing systemic threats to the economy. At the same time, digital transformation enhances the efficiency of business processes and public administration, fosters innovative business models, strengthens cyber-resilience, and ensures deeper integration of the European market into global value chains.

In the early 2020s, the European Union introduced the concept of the twin transition, which emphasised that the integration of environmental and digital solutions creates conditions for enhanced adaptability and competitiveness. It equips the EU economy with systemic tools to counter global challenges and reduces vulnerability to external shocks, thereby reinforcing economic security and supporting long-term geopolitical stability [1].

The Green Deal and *A Europe Fit for the Digital Age* became the fundamental pillars of the EU's institutional policy in 2020–2024 and defined the strategic direction toward a sustainable and secure future.

The purpose of this study is to assess the progress made in achieving the target benchmarks of the EU's Strategic Development Plan for 2020–2024 within the priority areas of *A Green Deal* and *A Europe Fit for the*



Digital Age. This, in turn, makes it possible to substantiate the validity of the chosen policy course and to identify the challenges arising from delays in meeting specific indicators.

25.1. The European Green Deal: strategic objectives and outcomes in the context of the EU's environmental security

Powerful innovative instruments for enhancing the EU's climate and environmental security include the *ambitious European Green Deal* [2], the *broader Green Transition policies*, and the *new Clean Industrial Deal*, which continues – through institutional succession – the implementation of the objectives originally set under the Green Deal framework. These instruments have been developed in response to contemporary global challenges such as climate change, resource scarcity, and environmental threats to humanity. To better understand the specifics of implementing the EU's Strategic Agenda for 2025–2029 [3], as well as the new Clean Industrial Deal that extends the course set by the European Green Deal, it is essential to assess the progress made in achieving the targets established under the Green Deal priority during the previous EU institutional cycle. These targets were articulated, among other sources, in the Strategic Plans of the European Commission's directorates for 2020–2024 [4]. Identifying the degree of target achievement, along with the gaps between planned and actual indicator values, will help refine the green transition process by integrating the obtained results into the formulation of objectives for the coming years. This will contribute to the successful implementation of Green Transition policies and the strengthening of the EU's environmental security.

The European Green Deal, introduced by the European Commission in December 2019, is defined as a 'new growth strategy' [2] and aims to position the EU as a global leader in combating climate change and promoting resource efficiency, innovation, and sustainable competitiveness. It is designed to align environmental objectives with economic opportunities, assuming that the transition to a low-carbon economy will enhance the well-being of both businesses and citizens. The central idea of the Green Deal is the transformation of the EU into a climate-neutral economy by 2050. This overarching objective is supported by a set of specific targets, including reducing greenhouse gas emissions by 55% by 2030 compared to 1990 levels,

promoting biodiversity conservation, and advancing the implementation of the circular economy, among others.

To understand the specifics of implementing the EU Strategic Plan for 2024–2029, we have summarized the available results of achieving long-term strategic objectives under the Green Deal priority during the previous institutional cycle of 2020–2024. The analysis of the corresponding indicators, as of 2024 (or the latest available year), was carried out based on the Strategic Plans for 2020–2024 and the annual reports of the European Commission’s structural units (Directorates and Executive Agencies) for 2024 [4].

Table 25.1 presents the results of target indicators for the Green Deal priority over time, showing baseline values, intermediate values, target values, and reported data for 2023 and 2024 (the most recent values). This dataset allows not only an assessment of the outcomes but also the observation of indicator trends over time.

The analysis shows that greenhouse gas emissions decreased by 25% in 2018 compared to 1990, but only by 20% in 2020. However, following the implementation of a series of strategic documents, plans, and programs addressing climate change, emissions reductions reached 32.5% by 2022 and, according to preliminary estimates, 37% by 2023. These results indicate a high probability of achieving the long-term target of a 55% reduction in greenhouse gas emissions by 2030.

An important target indicator under the Green Deal priority ‘Protecting, Conserving and Restoring Biodiversity’ is the *Common Bird Population*. This indicator reflects the state of biodiversity and ecosystem integrity, showing the pressure exerted by human activity. Long-term trends indicate that between 1990 and 2022, the index of populations of 168 common bird species in the EU decreased by 14 points, and in 2023 the decline exceeded 15 points. EU member states need to significantly strengthen current policies and introduce new measures to ensure the recovery of populations and biodiversity overall.

A rapid improvement is observed in the *Pesticide Risk* indicator, which is based on the statistics of the number of chemical active substances in plant protection products available on the market. The index, which was 100 in 2016, decreased to 54 in 2022, approaching the target value of 50 by 2030. More recent data are currently unavailable.

Table 25.1

Achievement of target indicators under the Green Deal priority*

Indicator	Baseline (Year)	Interim milestone (Year)	Target (Year)	Reports 2023 ¹ (Year)	Reports 2024 ¹ (Year)
Net GHG emissions (changes in percent of the emissions compared to 1990 levels)	-25% net GHG emissions ² (2018)	-20% net GHG emissions (2020)	-55% net GHG emissions (2030)	-32,5% (2022)	-37% (2023)
Common birds population Index: 1990 = 100	88,00 (2018)	Curtail biodiversity loss (2020)	Curtail biodiversity loss (2024)	86,24 (2022)	85,03 (2023)
Pesticide risk Index: 2016 = 100	100 (2016)	73 (2020)	50 (2030)	54 (2022)	54 (2022)
Nitrate in groundwater	21,05 mg/l (2017)	Decrease (2020)	Decrease (2024)	20,51 mg/l (2021)	20,65 mg/l (2022)
Area under organic farming	7,99% (2018)	Increase (2022)	Increase (2024)	9,09% (2020)	10,5% (2022)
Size of the green economy	Gross value- added: €292797 mln Full-time equivalent employment: 4 503000 (2017)	Increase Increase (2022)	Increase Increase (2025)	€341218 mln 5 065000 (2020)	€368502 mln 5 065000 (2021)
Share of the environmental economy in the overall GDP in the EU	2.2% (2017)	Increase (2022)	Increase (2024)	2.53% (2020)	2.49% (2021)
Circular materials use rate	11.5% (2017)	Increase (2022)	Increase (2024)	11.5% (2022)	11,8% (2023)
Greenhouse gas emissions intensity of energy consumption Index 2000 = 100	86.9 (2017)	81.2 (2021)	Decrease (2022)	Decrease (2023)	83,6 (2024)
Climate-related economic losses	Total losses: EUR 13492 mln. Average losses over 30 years pro capita: € 30,26 (2017)	Decrease (2022)	Decrease (2024)	Total losses: €17657 mln. Average losses over 30 years pro capita: € 39,5 (2022)	Total losses: €20107mln. Average losses over 30 years pro capita: €44,84 (2022)
Proportion of climate related spending in the EU budget (MFF ³)	21% ⁴ (2014-2020, previous MFF)	n/a ⁵	30% (2021-2027, current MFF)	32.6% (2023)	34.32% (2024)
Level of average CO2 emissions from new cars (NEDC, WLTP)	20.4 g CO2/km (NEDC) (2018)	95 g CO2/km (NEDC) or 115.14 g CO2/km (WLTP) (2020)	95 g CO2/km (NEDC) or 115.14 g CO2/km (WLTP) (2024)	108.1 g CO2/km (WLTP) (2022)	106.6 g CO2/km (WLTP) (2023)

Table 25.1 (continued)

Level of average CO2 emissions from new vans (NEDC, WLTP)	158,1 g CO2/km (NEDC) (2018)	147 g CO2/km (NEDC) or 189.92 g CO2/km (WLTP) (2020)	147 g CO2/km (NEDC) or 189.92 g CO2/km (WLTP) (2024)	183,8 g CO2/km (WLTP) (2022)	180,8 g CO2/km (WLTP) (2023)
Share of renewable energy in gross final energy consumption, %	19,1 (2018)	20,0 (2020)	32,0 (2030)	23,0 (2022)	24,5 (2023)
Number of EU Ecolabel Products	77 358 products (2019)	Increase (2022)	Increase (2024)	88 921 products (2023)	98 977 products (2024)
Eco-Innovation Index 2013 p. = 100	109,44 (2018)	Increase (2022)	Increase (2024)	121,47 (2022)	127,5 (2024)
Municipal waste generation and treatment	Generation of municipal waste: 504 Kg/person Recycling & composting: 47.2% Landfilling: 24.6 (2019)	n/a	Generation of municipal waste (2024): Reduce Recycling & composting: 50% ⁶ . Landfilling: reduce (to 10% by 2035) ⁷	Generation of municipal waste: 513 Kg/person. Recycling & composting: 48.5%. Landfilling: 23% (2022)	Generation of municipal waste: 513 Kg/person. Recycling & composting: 48.5%. Landfilling: 23% (2022)

¹Latest known value

²Greenhouse gas emissions (GHG) – the difference between the amount of greenhouse gas produced and the amount removed from the atmosphere.

³MFf (multiannual financial framework) – the long-term EU budget, usually covering a 7-year period.

⁴Evaluation based on commitment appropriations

⁵n/a - there are no annual targets: between 2021-2027 expenditure is expected to fluctuate over the years

⁶65% by 2035.

⁷The targets indicated for 2035 by Waste Framework Directive 2024.

*Source: compiled by the authors based on [4]

The long-term trend in *nitrate content in groundwater* is also favorable, decreasing from 21.05 mg/L (2017) to 20.51 mg/L (2021), although in 2022 this indicator slightly worsened to 20.65 mg/L.

The area under *organic farming* has shown steady growth, increasing from 7.99% in 2018 to 9.09% in 2020 and 10.5% in 2022.

The *size of the green economy* reflects the contribution of economic sectors producing environmental products. The *Environmental Goods and Services Sector (EGSS)* refer to the part of the economy that produces environmental products – goods and services aimed at environmental protection or resource management [5]. Products and services for environmental protection prevent, reduce, or eliminate pollution or any other

environmental degradation. This also includes measures aimed at restoring degraded habitats and ecosystems. Examples include electric vehicles, catalytic converters and filters to reduce pollutant emissions, wastewater and waste treatment services, and noise insulation works.

Products and services for resource management protect natural resource stocks from depletion. Examples include renewable energy production, energy-efficient and passive buildings, seawater desalination, and rainwater harvesting [6].

The size of the green economy is measured by two indicators. *Gross value added (GVA)* represents the contribution of environmental goods and services production to the gross domestic product, in millions of euros. *Employment* is measured in full-time equivalents in the production of environmental goods and services. In 2017, GVA amounted to €292,797 million, and full-time equivalent employment reached 4,503,000 persons. By 2020, these figures increased by 16.5% and 12.5%, reaching €341,218 million and 5,065,000 persons, respectively. In 2021, GVA further increased by €27,284 million to €368,502 million, with more recent data currently unavailable.

The share of the *green economy* in the total EU GDP was 2.2% in 2017. This indicator reflects the EU's progress toward the green transition. The growth of this share to 2.53% in 2020 and its slight decline to 2.49% in 2021 indicate a slow and uneven dynamic in the EU's green transition. In particular, the increase from 2.2% in 2017 to 2.53% in 2020 demonstrates some progress across various economic sectors, while the decrease to 2.49% in 2021 points to temporary setbacks in this transition.

An important component of the European Green Deal, the circular economy, is reflected in the indicator *Share of Circular Materials*. The Circular material use rate is defined as the ratio of circular material usage to total material usage. This indicator shows very slow dynamics: from 2017 to 2022, it remained at 11.5%, and only in 2023 did it increase to 11.8%.

The focus of the European Green Deal on reducing climate pressure is reflected in the indicator *Greenhouse Gas Emission Intensity of Energy Consumption*, calculated as the ratio of greenhouse gas emissions in the energy sector to total gross energy consumption. The index value in 2000 was 100, with a baseline value of 86.9 in 2017. Reports indicate a decrease in the index to 83.6 by 2024.

Economic losses related to climate change measure the financial impact of weather- and climate-related natural disasters, expressed as annual economic losses (in current values) and in euros per capita. Data are presented as smoothed time series based on 30-year moving averages rather than annual figures. Total losses in 2017 amounted to €13,492 million, with average losses of €30.26 per capita (over 30 years). In 2022, the indicator increased, with total losses of €17,657 million and average losses of €39.5 per capita. In 2023, the upward trend continued, with total losses reaching €20,107 million and 30-year average losses of €44.84 per capita.

The consideration of the *climate factor in the European Union budget* is reflected in the share of climate-related expenditures within the Multiannual Financial Framework (MFF) – the EU’s long-term budget, which typically covers a seven-year period. The baseline value was 21% for 2014–2020. No annual targets are set for this indicator; it is expected that expenditures from 2021 to 2027 will fluctuate annually, averaging around 30%. Estimates indicate that in 2023 the indicator reached 32.6%, and in 2024 – 34.32%. The assessment is based on so-called commitment appropriations.

Thanks to new *CO₂ standards*, by 2035 all new cars and vans registered in Europe will have zero emissions. As an intermediate step towards zero emissions, *the average emissions of new cars should be reduced by 55% by 2030, and those of new vans by 50% by 2030*. This trajectory is expected to ensure zero emissions from road transport by 2050.

According to available data, the *baseline average CO₂ emissions from new cars* in 2018 amounted to 20.4 g CO₂/km under the NEDC standard. By 2020, this value increased to 95 g CO₂/km under the NEDC or 115.14 g CO₂/km under the WLTP standard. This increase can primarily be attributed to the growth in the number of new vehicles. The target for 2024 was set at the 2020 level. However, in 2022, emissions rose to 108.1 g CO₂/km, and although in 2023 this indicator slightly decreased to 106.6 g CO₂/km, it still significantly exceeds the target level.

Regarding *new vans*, the baseline average CO₂ emissions in 2018 were 158.1 g CO₂/km (NEDC). By 2020, this value decreased to 147 g CO₂/km (NEDC) or 189.92 g CO₂/km (WLTP), which was also set as the target for 2024. By 2022, emissions rose to 183.8 g CO₂/km, and in 2023 they slightly decreased to 180.8 g CO₂/km. However, this still significantly exceeds the

2024 target and shows almost no progress toward achieving zero emissions by 2050, as well as the targets set for 2030.

The *share of renewable energy* in gross final energy consumption increased from 19.1% in 2018 to 23.0% in 2022 and 24.5% in 2023. This demonstrates steady progress toward the target value of 32% by 2030.

The *number of products with the EU Ecolabel* has consistently grown, from 77,358 products in 2019 to 88,921 in 2023 and 98,977 in 2024. This trend aligns with the target-oriented goal of increasing the indicator.

The *Eco-Innovation Index* was 100 in 2013, increased to 109.44 in 2018, and reached 121.47 in 2022. The upward trend continued, reaching a value of 127.5 in 2024, fully in line with the target direction. The index measures the effectiveness of eco-innovation in EU member states based on 12 indicators across five thematic areas: eco-innovation inputs, eco-innovation activities, eco-innovation outputs, resource efficiency, and socio-economic outcomes [7]. This approach provides a comprehensive view of the effectiveness of ecological innovations.

The dynamics of the indicator '*Generation and Recycling of Municipal Waste*' also align with the goals of the European Green Deal. The baseline value for municipal waste generation in 2019 was 504 kg per capita, with 47.2% recycled or composted and 24.6% landfilled. The recycling and composting target for 2024 is 50% and 65% by 2035, while landfill disposal should be reduced to 10% by 2035. In 2022, municipal waste generation was 513 kg per capita, recycling and composting reached 48.5%, and landfill disposal was 23%. More recent data are not yet available.

The analysis revealed that 13 out of 17 indicators overall met their target values, indicating a positive impact of the green transition on the ecological security of the European Union. The best results were achieved in areas related to *greenhouse gas emissions*, including emissions from electricity consumption, and in *EU budget funding* to counter adverse climate impacts. The share of renewable energy in gross final energy consumption and the share of the green economy in EU GDP are also steadily increasing. This demonstrates the EU leadership's prioritization of implementing highly ambitious goals for combating climate change and global warming.

In the agricultural sector, according to the established targets for 2030, the risk of pesticide use is steadily decreasing. There is also a trend toward

reduced nitrate content in groundwater and an increase in areas under organic farming. Although quantitative targets for 2024 and beyond have not been set for these indicators, the latest available results as of 2022 showed positive dynamics.

The growth in the *share of circular materials* remains rather formal, reaching only 0.3% in 2023 compared to the 2017 baseline.

The increase, according to the set goals, in the *size of the green economy* and its share in the EU GDP demonstrates progress in the European economic green transition. The number of products with *EU Ecolabel certification* continues to rise. In addition, the positive trend in the *Eco-Innovation Index* indicates improvements in the innovation foundations of the green transition.

Achievement of the targets for these indicators reflects the effectiveness of the EU's Green Deal policy and confirms the advisability of maintaining the current trajectory of these indicators when implementing the goals and objectives of the EU Strategic Development Plan for 2024–2029.

At the same time, four indicators – the *Common birds population*, *Economic losses related to climate change*, *Average CO₂ emissions from new cars*, and *Average CO₂ emissions from new vans* – lag behind their target values, and experts express doubts about achieving the 2030 targets.

The outlined results of the green transition are directly correlated with an increase in environmental security in the European Union. Systematic reduction of greenhouse gas emissions, expansion of the share of renewable energy, and development of the green economy reduce the EU's dependence on fossil fuels and enhance the resilience of the energy system to external risks. This creates conditions for strengthening the EU's energy autonomy, which is a key element of its environmental and economic security amid growing geopolitical challenges.

Progress in agriculture is also of particular importance, as the reduction of pesticide use and nitrate content in groundwater directly affects environmental quality, food safety, and public health. Expansion of organic farming areas creates safer and more environmentally responsible production chains, aligning with the 'Farm to Fork' strategy. These measures contribute not only to environmental protection but also to establishing long-term guarantees for food security.

At the same time, the indicators that are lagging highlight the need to strengthen measures for biodiversity protection and climate risk adaptation. The decline in the population of common birds serves as a marker of ecosystem degradation, which may have long-term negative consequences for the stability of the natural environment. Economic losses from climate change indicate the EU's vulnerability to extreme weather events, while delays in reducing emissions from road transport underline the need for an accelerated transition to electric mobility and the development of sustainable transportation.

Thus, the European green transition is not only a tool for achieving climate goals but also a fundamental prerequisite for the EU's environmental security. The progress achieved confirms that the Green Deal strategy has a systemic impact on reducing environmental risks, enhancing the resilience of the economy and society to external threats, and ensuring sustainable development. Continued achievement of the target indicators set out in the EU's strategic documents will be a key factor for a safe and environmentally responsible future.

25.2. Europe's strategic priorities on the path to the digital age

Digital transformation in the contemporary context is considered a key factor for socio-economic development and national security [13, p. 519]. For the European Union, the development of a digital economy and a digital society is one of the strategic objectives aimed at ensuring sustainable economic growth, fostering innovation, and enhancing competitiveness. In this regard, the priority 'A Europe Fit to the Digital Age' was included in the Strategic Agenda for 2020–2024 [14].

In 2021, the European Commission proposed the Europe's Digital Decade initiative [15], which set specific targets for Europe's digital transformation by 2030. This initiative is guided by the EU's Digital Economy and Society Transformation Plan – the 'Digital Compass for 2030' [16]. Digital transformation focuses on creating an innovative, human-centered, and secure digital ecosystem and involves a set of measures aimed at forming a unified digital space, which includes: the development of digital skills among the population, the establishment of secure and efficient digital

infrastructure, support for the digital transformation of the business sector, and the digitalization of public administration and government services [17].

The European Union's Digital Single Market Strategy [18] was launched in 2015 and aimed to promote economic growth, increase employment, enhance competition, and foster investment and innovation in the EU, based on three pillars:

1. Better access for consumers and businesses to digital goods and services across Europe.
2. Creating appropriate and equal conditions for the development of digital networks and innovative services.
3. Maximizing the growth potential of the digital economy.

To better understand the implementation pathways of the EU Digital Single Market Strategy and the achievement of digital targets by 2030, it is advisable to analyze the accomplishments within the priority "A Europe Fit to the Digital Age" for the period 2020–2024. Evaluating the achievement of these goals is important for assessing the effectiveness of the digital strategy and identifying challenges that remain relevant through 2030.

The authors have summarized the results of achieving the long-term strategic objectives under the priority 'A Europe Fit to the Digital Age' during the 2020–2024 institutional cycle. The analysis of the relevant indicators, as of 2024 (or the latest available year), was carried out based on strategic documents of the European Commission [4].

Table 25.2 presents the results of achieving the target values of indicators under the priority 'A Europe Fit to the Digital Age' as of 2024 (or the latest available period) and for previous years. This allows for the assessment of the extent to which the goals have been achieved over time, as well as identifying any deviations from the target values.

The Digital Economy and Society Index (DESI) is a composite index that, from 2014 to 2022, summarized Europe's digital performance and tracked the progress of EU countries in digital competitiveness. The DESI was calculated as a weighted average of five main dimensions: connectivity (25%), human capital (25%), use of the Internet (15%), integration of digital technologies (20%), and digital public services (15%). Higher values indicate better performance. The index value increased from 43.1 in the baseline year 2019 to 52.3 in 2022.

Table 25.2

Achievement of target indicators under the Europe fit to the digital age priority*

Indicator	Baseline (Year)	Interim milestone (Year)	Target (Year)	Reports 2023 ¹ (Year)	Reports 2024 ¹ (Year)
Digital Economy and Society Index, DESI	43,1 (2019)	Increase (2022)	Increase (2024) ¹	52,3 (2022)	52,3 (2022)
% of SMEs engaged in cross-border online trade	8,29% (2019)	Increase (2022)	Increase (2024)	8,73% (2022)	8,73% (2022)
Digital Skills	Basic Digital Skills: 54% (2021)	63% (2022)	67% (2024) ²	55,5% (2023)	55,6% (2023)
Share of people using digital technologies for learning	21% (2019)	Increase (2022)	Increase (2024)	31% (2023)	34,1 (2024)
Share of Erasmus+ participants who improved their digital skills while participating in the programme	60% 2019	Increase (2022)	Increase (2024)	53 2023	65,1% 2024
A digitally skilled workforce	13 (2018)	20 (2022)	27 (2024) ³	27 (2022)	27 (2024)
Users of the new Europass platform for learning and career management	- 72 000 visits per day - registered users (2018)	80 000 1 000 000 (2022)	95 000 2 500 000 (2024)	57 730 5 500 000 (2023)	63 520 7 562 180 (2024)
Share of companies using artificial intelligence	7,6% (2021)	Increase (2022)	Increase (2024)	8% (2023)	13,5 (2024)
Businesses that sell online	17,4 (2019)	Increase (2022)	Increase (2024)	19,74 (2023)	20,75% (2024)
Businesses with access to broadband internet of at least 100 Mbps	46% (2020)	Increase (2022)	Increase (2023)	60% (2023)	65 (2024)
Broadband Internet access ⁴ (households)	2 989 418 (2018)	Increase (2022)	11 311 160 (2023)	7 883 327 (2022)	7 883 327 (2022)
Digitalization costs	EUR 2.936 bln (2019)	Increase	EUR 15.3 bln for 2014-2020 (+20 bln planned for 2021-2027)	EUR 13.9 bln spent in 2014-2020 ⁵	EUR 13.9 bln spent in 2014-2020
Coverage of European Commission staff by the cybersecurity program, %	15% (employees undergo training once every 7 years) (2019)	25% (employees undergo training once every 4 years) (2022)	35% (employees undergo training once every 3 years) (2024) ¹	36% (2023) ⁶	35% Target achieved (2024) ⁷

Table 25.2 (continued)

Time to resolve security incidents	17 working days (2020)	15,3 (-10%) (2022)	13,6 (-20%) (2024) ¹	16,6 working days	Target exceeded (2024) ⁸
Number of EU institutions using the cloud broker service	21 (end of 2019)	30 (2022)	60 (2024) ¹	64 (31.12.2023)	67 Target exceeded (2024)
Number of information systems connected to the digital service managed by the European Commission	40% (2020)	46% (2022)	52% (2024) ¹	57% (2023)	Target achieved (2024)
Overall level of end-user satisfaction with the digital workplace solutions provided DIGIT	End-user satisfaction level above 80% (end of 2019) ⁹	Above 80% (2022)	Above 80% (2024) ¹	91% Target exceeded	94% Target exceeded

¹Latest known value²Target set by DIGIT in the Strategic Plan for 2020-2024.³Встановлено на базі цілей на 2025³Set based on the European Skills Agenda 2025 targets (70%)⁴The European Digital Competence Framework is planned to be used by all Member States⁵Additional households with broadband access of at least 30 Mbps⁶For the period 2021-2027, the amount of costs will be known at a later stage of implementation⁷Average participation rate in all 3 Cyber Aware – Security Education Programme 2023 training events: 36%⁸35% of staff have completed online training on the Cyber Aware Security Education Programme⁹Target exceeded, in particular due to automation¹⁰Target set in the previous Strategic Plan

*Source: compiled by the authors based on: [4]

Starting in 2023, according to the Europe's Digital Decade policy program for 2030, DESI has been integrated into the Digital Decade Dashboard [19] and is used to monitor progress in achieving digitalization goals. Therefore, after 2022, DESI values were no longer updated in the European Commission reports analyzed here. Nevertheless, the achieved results clearly indicate significant progress in this area.

As shown by the analysis results, the *share of small and medium-sized enterprises (SMEs) engaged in cross-border online trade* increased from 8.29% to 8.73% between 2019 and 2022 (the latest available value reported), in line with the set objectives. This indicator combines the use of digital technologies with the internationalization of SMEs and thus measures SME

progress in two key areas simultaneously: internationalization and digitalization.

The *Digital Skills* indicator reflects the ability of individuals aged 16 to 74 to perform online activities in five specific areas: information and data literacy, communication and collaboration, problem-solving, safety, and content creation. It is calculated every two years (in each odd-numbered year) as an assessment of individual digital skills on a scale of: none, limited, narrow, low, basic, or above basic. To be considered digitally proficient at a basic level, individuals must be able to perform at least one activity in each area. In 2021, the share of people demonstrating basic digital skills was 54%. In 2023, this figure slightly increased to 55.6%, which remains significantly below the interim target of 63% for 2022 and the goal of 67% for 2024.

The share of people using digital technologies for learning (relating to programs funded under Erasmus+) rose from 21% in the baseline year 2019 to 34.1% in the reporting year 2024. This indicator measures the proportion of individuals who use online courses, educational materials, or communicate with teachers or fellow students via educational websites/portals, reflecting progress toward the objective of increasing the use of digital technologies in teaching and learning to support quality and inclusive education.

The achievement of this goal is also evidenced by the increase in the *share of Erasmus+ participants who improved their digital skills during their participation in the programme*, from 60% in 2019 to 65.1% in 2024. This indicator measures the share of Erasmus+ participants who stated that they improved their digital skills through their participation in the Erasmus+ programme. The current dynamics correspond to the target for increasing the indicator set out in the European Commission's strategic plans for the period 2019–2024.

Digitally qualified workforce: This indicator is defined as the number of EU Member States implementing the European Digital Competence Framework. While in 2018 only 13 countries applied the framework, by 2022 all 27 EU Member States were covered.

It was found that the *usage level of the Europass platform for learning and career management* does not meet all target values. Europass is one of Europe's most visited websites and an effective tool created by the EU to support career development and employment for the general public. The

number of platform visits and registered users are key indicators of Europass's popularity and impact. In 2018, the platform recorded 72.000 daily visits. Although the target for registered users in 2024 was significantly exceeded, reaching 7.562.180, the daily visits decreased compared to the baseline year to 63.520, suggesting that the set target may have been insufficiently justified or realistic.

The share of companies using artificial intelligence almost doubled between 2021 and 2024, increasing from 7.6% to 13.5%, indicating progress in implementing the strategic plan in this area.

Similarly, *the share of enterprises conducting online sales* increased from 17.4% in 2019 to 20.75% in 2024. This indicator measures the percentage of enterprises (with 10 or more employees) generating at least 1% of their turnover from online sales.

Important indicators reflecting the level of digital transformation in the economy and society include internet access for enterprises and households. *The share of enterprises with broadband internet access of at least 100 Mbps* showed a strong positive trend, reaching 60% in 2023 and 65% in 2024, compared to 46% in 2020. This indicator measures the percentage of enterprises (with 10 or more employees) whose internet connection provides a maximum recorded download speed of at least 100 Mbps.

The number of additional households with broadband access of at least 30 Mbps increased from 2,989,418 in 2018 to 7,833,327 in 2022, which fell short of the target set for 2023, amounting to 11,311,160 households.

Expenditures on digitalization within the EU budget for 2014–2020 amounted to EUR 2.936 billion as of 2019. The target for the 2014–2020 period was set at EUR 15.3 billion (+EUR 20 billion was planned for 2021–2027 under the MFF budget). During 2014–2020, a total of EUR 13.9 billion was spent. The total expenditures for the 2021–2027 period will be reported later.

Resilience to cybersecurity threats, which are constantly emerging in today's world, is assessed, in particular, through the *coverage of European Commission personnel by the cyber awareness program*. In 2024, the target set in the 2020–2024 strategic plan was fully achieved, according to which 35% of personnel completed the online training under the Cyber Aware Security Education Programme.

According to the report of the Directorate General for Digital Services (DIGIT) of the European Commission, the target for 2024 regarding *the time required to resolve security incidents* was exceeded. The baseline value as of 2020 was 17 working days. The 2024 strategic plan set a target to reduce this time by 20% to 13.6 working days. However, in 2023, only a slight reduction to 16.6 working days was recorded. The 2024 DIGIT report notes that, although the total number of security incidents per year remained relatively stable in 2022 and 2023, the number of incidents related to public cloud services increased significantly. Resolving such issues depended on external resources, which affected the indicator. Throughout 2024, improvements in security controls for cloud services helped to compensate for this lag [4].

The number of EU institutions using the cloud broker service is one of the indicators reflecting resilient public administration with effective digital infrastructure and corresponding digital workplaces [4]. During the period 2019–2024, the number of institutions increased from 21 to 67, thus exceeding the target of 60 institutions set in the Strategic Plan.

Another indicator of an effective digital structure in public administration is *the number of information systems connected to the digital service managed by the European Commission*. The target level of 52% was exceeded in 2023, when the share of such systems reached 57%.

Finally, the *overall level of end-user satisfaction with digital workplace solutions* completes the list of digitalization indicators. This measure exceeded 80% in 2019 and reached 94% in 2024, surpassing the target set in the 2020–2024 Strategic Plan.

Thus, out of the 17 indicators examined, 14 fully achieved or exceeded the established targets. This primarily concerns the development of digital infrastructure, the integration of digital technologies into business activities, the growth of e-commerce, the adoption of artificial intelligence, the digitalization of public administration, and the improvement of digital workplace quality. Positive trends were also observed in indicators related to Erasmus+ educational programs and the development of digital skills in the EU workforce. These results demonstrate the systematic nature of the EU's digital policy, which addresses both economic and social dimensions.

The analysis indicates an overall high level of achievement of the objectives set in the 2020–2024 Strategic Agenda, confirming the

effectiveness of the chosen digital strategy and the appropriateness of continuing along the established path toward digital transformation.

At the same time, a number of problematic aspects were identified that require additional attention. In particular, the indicators for basic digital skills among the population and household coverage with high-speed broadband internet did not reach the planned targets, which may pose risks to digital inclusion and limit the effective use of advanced technologies. The indicator related to the use of the Europass platform was also only partially achieved.

Achieving the objectives by 2030 will require strengthened efforts to develop digital skills among the population, expand access to high-speed internet, enhance the effectiveness of digital services, and increase investments in cybersecurity. This will help improve the efficiency of digital transformation and reduce risks such as cyber threats, misinformation, and privacy breaches.

Thus, the assessment results overall indicate significant progress by the European Union toward a “dual” green and digital transformation, while simultaneously highlighting several strategic challenges that require comprehensive long-term solutions.

References

1. The twin green & digital transition: How sustainable digital technologies could enable a carbon-neutral EU by 2050. Available at: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/twin-green-digital-transition-how-sustainable-digital-technologies-could-enable-carbon-neutral-eu-2022-06-29_en

2. Communication from the commission. The European Green Deal. *European Commission*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2019%3A640%3AFIN>

3. Strategic agenda 2024-2029. *European Commission*. Available at: <https://www.consilium.europa.eu/en/european-council/strategic-agenda-2024-2029/>

4. Strategic Documents. *European Commission*. Available at: https://commission.europa.eu/strategy-and-policy/strategy-documents_en

5. Environmental goods and services sector accounts. Practical guide. 2016 ed. Eurostat. Available at: <https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/KS-GQ-16-011>

6. Environmental goods and services sector. Data description. Eurostat. Available at: https://ec.europa.eu/eurostat/cache/metadata/en/env_egs_esms.htm

7. EU Eco-Innovation Index 2024. Publication Office of the European Union. Available at: <https://op.europa.eu/en/publication-detail/-/publication/afe9989d-95ac-11ef-a130-01aa75ed71a1/language-en>

8. Environmental security. Competence Centre on Foresight. *European Commission*. Available at: https://knowledge4policy.ec.europa.eu/foresight/topic/changing-security-paradigm/environmental-security_en

9. Enhancing climate security and defence. European Union External Act. Available at: https://www.eeas.europa.eu/eeas/enhancing-climate-security-and-defence_en#:~:text=The%20EU%20approach%20to%20climate%20and%20security.,Communication%20and%20called%20for%20its%20swift%20implementation.

10. EU energy autonomy and climate targets – the next ten years. May 25, 2023. Available at: <https://euauditors.medium.com/eu-energy-autonomy-and-climate-targets-the-next-ten-years-39739f0bede5#:~:text=For%20the%20energy%20sector%2C%20open%20strategic%20autonomy,overall%20energy%20mix%2C%20and%20strengthening%20international%20cooperation.>

11. Transport, Telecommunications and Energy Council (Energy), 16 June 2025. European Council. Available at: <https://www.consilium.europa.eu/en/meetings/tte/2025/06/16/>

12. Farm to Fork strategy. *European Commission*. Available at: https://food.ec.europa.eu/horizontal-topics/farm-fork-strategy_en

13. Гомотюк А., Мажук В., Батюк О., Сіранчук В. Цифрова трансформація як фактор розвитку: виклики для економіки та суспільства. Економічний аналіз. 2024. Т. 34. № 4. С. 511–522. <https://doi.org/10.35774/econa2024.04.511>

14. A Europe Fit to the Digital Age. *European Commission*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en

15. Europe's Digital Decade. *European Commission*. Available at: <https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

16. 2030 Digital Compass: the European way for the Digital Decade. EUR-Lex. Available at: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118>

17. Europe's Digital Decade: digital targets for 2030. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

18. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. Brussels, 6.5.2015 COM(2015) 192 final. *European Commission*. Available at:

https://ec.europa.eu/commission/presscorner/api/files/attachment/8210/DSM_communication.pdf

19. DESI dashboard for the Digital Decade. Available at: <https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts>

Section 6
**Integration of Ukraine into the European
Economic and Political-Legal Space**

Chapter 26
***Methodological approaches to enhancing the effectiveness of
integration processes within the EU economic and political-
legal space***
(V. Ustymenko, R. Dzhabrailov, T. Hudima)

The rule of law, as a fundamental legal value and a core legal category, is deeply embedded in the constitutional and legal fabric of national legal orders and constitutes an integral foundation of international law and of the legal systems of supranational entities.

It is no coincidence that the EU integration process is structured in such a way that Ukraine's accession negotiations commence and conclude with the fulfilment of tasks and compliance with reform benchmarks set out in the roadmaps prepared by Ukraine within Cluster 1, 'Fundamentals of the Accession Process to the European Union'. In particular, the media have highlighted Roadmap for the Rule of Law, the functioning of democratic institutions, public administration reform, as well as an action plan for ensuring the protection of the rights of persons belonging to national minorities (communities) of Ukraine [1–4].

The special role of reforms within Cluster 1, 'Fundamentals of the EU Accession Process', is determined by the prevalence of a value-based approach, which assumes a constitutive, paradigmatic, and system-forming character. The development of contemporary national legislation oriented towards the legal values of the European Union serves as a meaning-forming driver of legal reforms and of changes in state legal policy. In this context, law-making activity acquires particular significance, as it should facilitate the drafting and adoption of normative legal acts aligned with EU law.

The examination of these issues constitutes the objective of this chapter.

26.1. The Principle of the Rule of Law as a Fundamental Legal Value and a Foundation of European Integration Processes

The rule of law is explicitly mentioned among the values upon which the European Union is founded, as reflected in Article 2 of the Treaty on European Union, a constituent act of EU primary law, which provides as follows: ‘The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail’ [5].

Compliance with the values enshrined in Article 2 of the Treaty on European Union constitutes a condition for a European State to submit an application for membership of the European Union. This provision is codified in Article 49(1) of the Treaty on European Union, which stipulates: ‘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’ [5].

In the publication ‘Introduction to the Political System of the European Union’, A. Parol draws attention to the consequences of breaches of EU values, placing particular emphasis on the comprehensive nature of the measures employed by the European Union to ensure compliance with the principle of the rule of law. Among such measures, the author identifies instruments of judicial and political oversight, notably the possibility of lodging a complaint before the Court of Justice of the European Union for a Member State’s failure to fulfil its obligations under the Treaties, as well as the application of the procedures laid down in Article 7 of the Treaty on European Union and the conditionality mechanism governing access to funds from the EU budget [6, p. 58].

At the same time, the procedure laid down in Article 7 of the Treaty on European Union consists of two interrelated stages, which may be characterised as preventive and protective, depending on the degree of seriousness of the breach of the values referred to in Article 2 TEU and the duration of such a breach.

In particular, the preventive function of the measures provided for in Article 7(1) TEU lies in the issuance of appropriate recommendations to a Member State where there is a clear risk of a serious breach of those values.

Conversely, the existence of a serious and persistent breach of the values enshrined in Article 2 TEU gives rise to the application of protective measures, which consist in the suspension of certain rights of the Member State concerned deriving from the application of the Treaties, including the voting rights of the representative of the Member State's government in the Council (Article 7(3) TEU) [5].

Where the application of Article 7 of the Treaty on European Union is possible, including in situations where the breach manifests itself both in areas governed by EU law and in areas falling within the exclusive competence of the Member States (the autonomous level) (as clarified in point 1.1 of section 1 of the European Commission Communication to the Council of the European Union and the European Parliament on Article 7 of the Treaty on European Union – Respect for and Promotion of the Values on Which the Union Is Founded) [7], the application of the protective mechanism enshrined in Article 258 of the Treaty on the Functioning of the European Union is limited to cases in which a breach of EU values takes the form of non-compliance with specific provisions of EU law, as set out in point 3 of the European Commission Communication to the European Parliament and the Council, 'A New EU Framework to Strengthen the Rule of Law'.

In particular, the European Commission may bring an action before the Court of Justice of the European Union where it considers that a Member State has failed to fulfil an obligation under the Treaties and has not complied with the reasoned opinion issued by the European Commission (Article 258 of the Treaty on the Functioning of the European Union). Where the Court of Justice of the European Union finds that a Member State has failed to fulfil its obligations under the Treaties, that State is required to take the necessary measures to comply with the judgment of the Court. If the Court finds that the Member State concerned has failed to comply with the judgment of the Court, it may impose on that State the obligation to pay a lump sum or a penalty payment. In this context, the European Commission determines the amount of the lump sum or penalty payment to be paid by the Member State concerned, which the Commission considers appropriate in the circumstances. This specific sequence of actions by the European Commission and the Court of Justice of the European Union is laid down in Article 260 of the Treaty on the Functioning of the European Union [5].

The practice of applying financial sanctions against a Member State as a consequence of breaches of the principle of the rule of law has developed gradually and has gained its greatest resonance within the framework of the

conditionality mechanism, which, as noted by A. Parol, is also referred to as ‘money for the rule of law’. [6, p. 215]. The foundations of this mechanism were laid down in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of the European Union of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (hereinafter – Regulation 2020/2092) [9].

As stated in recital 7 of Regulation (EU, Euratom) 2020/2092, whenever Member States implement the Union budget, including resources made available through the Recovery Instrument of the European Union established pursuant to Council Regulation (EU) 2020/2094, as well as through loans and other instruments guaranteed by the Union budget, and irrespective of the method of implementation applied, respect for the rule of law constitutes an essential precondition for compliance with the principles of sound financial management laid down in Article 317 of the Treaty on the Functioning of the European Union. The significantly broader role of the rule of law in fostering the development of the economies of the Member States and in strengthening democratic regimes is emphasised in recital 11 of Regulation 2020/2092, which underlines that respect for the rule of law is of fundamental importance not only for Union citizens, but also for business initiatives, innovation, investment, economic, social and territorial cohesion, as well as for the proper functioning of the internal market, which is most likely to flourish where a strong legal and institutional framework exists. In this context, recital 13 of Regulation 2020/2092 proclaims the existence of a clear link between respect for the rule of law and the effective implementation of the Union budget in accordance with the principles of sound financial management.

The normative enshrinement of the legal link between compliance with the principle of the rule of law and the ability to dispose of funds allocated to Member States from the EU budget was subsequently recognised as legitimate in the judgments of the Court of Justice of the European Union in Case C-156/21, *Hungary v Parliament and Council*, ECLI:EU:C:2022:97, and Case C-157/21, *Poland v Parliament and Council*, ECLI:EU:C:2022:98.

Attempts by Hungary and Poland to secure the annulment of Regulation (EU, Euratom) 2020/2092, substantiated by claims that the European Union had exceeded its competences and infringed the principle of legal certainty, as noted in the handbook ‘The Case Law of the Court of Justice of the European Union on the Rule of Law and Its Significance for Ukraine’,

prepared by T. Komarova and A. Łazowski, did not find support from the Court of Justice of the European Union [10, p. 47–50].

The authors of the aforementioned handbook set out a number of important conclusions reached by the Court of Justice of the European Union when examining the actions brought by Hungary and Poland, namely [10, c. 47–49]:

- Regulation (EU, Euratom) 2020/2092 is aimed at protecting the Union budget against the consequences resulting from breaches of the principle of the rule of law and does not constitute a sanction for such breaches as such;

- compliance with the values laid down in Article 2 of the Treaty on European Union cannot be reduced to an obligation that a candidate State must fulfil solely in order to accede to the European Union and which it may disregard after accession;

- the horizontal ‘conditionality mechanism’ established by Regulation 2020/2092, which makes access to funding from the Union budget conditional upon a Member State’s compliance with the principle of the rule of law, may fall within the competences conferred by the EU Treaties to lay down financial rules relating to the implementation of the Union budget;

- the procedure under Article 7 of the Treaty on European Union and the procedure established by Regulation 2020/2092 pursue distinct objectives.

Drawing conclusions from the analysis of the positions adopted by the Court of Justice of the European Union in the cases brought by Hungary and Poland, T. Komarova and A. Łazowski synthesise a set of important recommendations that are useful for consideration in national law-making and law-enforcement practice, namely [10, p. 49–50]:

- the judgments of the Court of Justice of the European Union are important for understanding that the principle of the rule of law constitutes a “strictly legal”, rather than a ‘purely political’, concept that is common to all Member States of the European Union. The same applies, to an equal extent, to candidate States for EU membership, which undergo a screening process assessing compliance with the principle of the rule of law.

In addition to this conclusion, emphasis may be placed on the importance of demonstrating genuine compliance with the principle of the rule of law and its practical applicability. In particular, this is ensured by the key provisions of Cluster 1, ‘Fundamentals of the EU Accession Process’, through the prism of which the degree of compliance with the Copenhagen

criteria for EU accession is assessed, and which are explicitly referred to in recital 4 of Regulation (EU, Euratom) 2020/2092;

- references to national identity cannot be used to justify derogations from the general principle of the rule of law. On the contrary, respect for the rule of law constitutes a clear legal obligation under EU law, rather than a merely political commitment;

- EU values are relevant not only at the stage of a State's accession to the European Union, but throughout the entire period of its membership. This reflects the so-called principle of 'irreversibility' with regard to respect for the rule of law.

In further elaboration of this caveat, it is important to note that recital 5 of Regulation (EU, Euratom) 2020/2092 emphasises that the laws and practices of the Member States must continue to comply with the common values on which the Union is founded.

It is appropriate to concur with T. Komarova and A. Łazowski that the aforementioned judgments of the Court of Justice of the European Union in the cases brought by Hungary and Poland make it possible to fully appreciate the role of the principle of the rule of law in ensuring the legal order and its systemic interconnection with other fundamental values of the European Union.

The case-law of the Court of Justice of the European Union undoubtedly plays an important role in enhancing the quality of both law-making activity and law-enforcement practice. Where a breach of the principle of the rule of law occurs at the stage of drafting a legal norm or in the course of its application, the task of restoring the regulation of social relations in conformity with justice as one of the fundamental principles of law, as emphasised in the decision of the Constitutional Court of Ukraine of 2 November 2004 No. 15-rp/2004 in the case concerning the imposition by a court of a more lenient penalty (subparagraph 4.1 of paragraph 4 of the reasoning part) [11], should be ensured by an effective judiciary, which must prevent arbitrariness where it is committed by the State acting through its public authorities.

In the Venice Commission Report No. 512/2009, 'The Rule of Law', adopted at its 86th Plenary Session on 25–26 March 2011, the Ukrainian translation of which was prepared by S. Holovaty, paragraph 37 sets out eight 'ingredients' of the rule of law, which include: (1) legality, in the sense that the law must be accessible, clear and foreseeable; (2) legal certainty, meaning that questions of legal rights should be resolved by law and not on the basis

of discretion; (3) equality before the law; (4) the lawful, fair and reasonable exercise of power; (5) protection of human rights; (6) access to justice, ensuring the availability of mechanisms for resolving disputes without excessive costs or undue delay; (7) a fair trial; (8) compliance by the State with its obligations under international law as well as those arising from national law [12].

Consistent with the understanding of the Venice Commission, the Court of Justice of the European Union, and the European Court of Human Rights regarding the substantive content of the rule of law is the framework of core principles outlined by the European Commission, which are intended to elucidate the essence of the rule of law as one of the common values of the European Union referred to in Article 2 of the Treaty on European Union.

In particular, the European Commission Communication to the European Parliament and the Council, 'A New EU Framework to Strengthen the Rule of Law', identifies the following principles: legality, encompassing a transparent, accountable, democratic and pluralistic law-making process; legal certainty; prohibition of arbitrariness by the executive authorities; independence and impartiality of the judiciary; effective judicial review, including with regard to respect for fundamental rights; and equality before the law.

The aforementioned Communication further emphasises that the principles listed above serve as instruments for ensuring compliance with and respect for democracy and human rights. Accordingly, the rule of law constitutes a constitutional principle encompassing both formal and substantive elements (paragraph 2).

In developing its understanding of the systemic interconnections between the rule of law and other values, the European Commission concludes that respect for the rule of law is closely linked to respect for democracy and fundamental rights: it is impossible to ensure democracy and the protection of human rights without respect for the rule of law, and vice versa. Fundamental rights can be effective only where they are subject to judicial protection (paragraph 2 of the European Commission Communication to the European Parliament and the Council of the European Union, 'A New EU Framework to Strengthen the Rule of Law') [8].

It is therefore no coincidence that the Charter of Fundamental Rights of the European Union proclaims democracy and the rule of law as the foundations of the Union (second recital of the Preamble) [13].

The Roadmap for the Rule of Law presented by Ukraine, which defines a comprehensive set of reforms within the negotiation process for Ukraine's accession to the European Union under Negotiation Chapters 23, 'Judiciary and Fundamental Rights', and 24, 'Justice, Freedom and Security', places particular emphasis on human rights as an integral element of a democratic regime, the safeguarding and protection of which are possible only where the rule of law is respected.

In particular, among the strategic outcomes of the Roadmap for the Rule of Law, as presented in point 3.1 'Human Rights Framework' of Section III 'Fundamental Rights', the following objective is envisaged: 'Ensuring compliance of national legislation and mechanisms for the protection of human rights and freedoms with the standards of the European Union and the provisions of the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights'. The achievement of this objective is to be supported by a set of measures, including, *inter alia*, the drafting and adoption of an Action Plan for the implementation of the National Human Rights Strategy, aimed, among other things, at addressing key challenges in ensuring the effective realisation of human rights under the legal regime of martial law and during the post-war recovery of Ukraine (subparagraph 1 of point 3.1 'Human Rights Framework' of Section III 'Fundamental Rights') [1].

Undoubtedly, under the legal regime of martial law, the task of ensuring and protecting human rights acquires existential significance, which necessitates the adoption by the State of effective measures to prevent and counter wartime threats in order to avert or minimise adverse consequences for individuals and for the sphere of their social, economic, environmental and other rights. At the same time, under conditions of martial law, the risks of human rights violations by public authorities and/or local self-government bodies are considerably higher, which significantly reinforces the role of the judiciary in restoring violated human rights.

At the same time, judicial practice in the adjudication of certain categories of disputes concerning the rights and legitimate interests of citizens demonstrates interpretations and applications of legislative acts in a manner that cannot be regarded as consistent with the principle of the rule of law, as is examined in greater detail in a separate authorial study [14].

26.2. Ideational and value-based approaches of the European Union as a basis for improving the national model of legislative drafting

The development of contemporary national legislation oriented towards the legal values of the European Union serves as a meaning-forming driver of legal reforms and transformations in state legal policy. In this context, law-making activity acquires particular significance, as it should facilitate the drafting and adoption of normative legal acts aligned with EU law.

The Constitution of Ukraine, as an act of the highest legal force within the national legal system, lays the foundation for law-making activity. Norms-framework, norms-principle, norms-presumptive, etc. [15, pp. 167–168] form a system of safeguards guiding the choice of methods and instruments of legislative drafting; their disregard signals the unconstitutionality of a normative legal act. Constitutional defects in a draft normative legal act that are not remedied at the drafting stage, once the act is adopted, acquire the characteristics of threats to the constitutional order of the State and to the fundamental rights and freedoms of the individual and the citizen.

Accordingly, progress in European integration will be constrained by the non-compliance of adopted normative legal acts with the principle of the rule of law as one of the fundamental values on which the European Union is founded, as enshrined in Article 2 of the Treaty on European Union as an act of EU primary law [5].

In contrast to threats of a hybrid nature, which, according to the definition contained in the Concept for Ensuring the National Resilience System approved by Presidential Decree of Ukraine No. 479/2021 of 27 September 2021 [16], ‘are of a latent nature or are disguised as other processes within the legal framework’, threats arising from the deliberate disregard of the provisions of the Constitution of Ukraine in law-making activity are evident and, as a rule, their detection and identification take place at the relevant stages of the legislative process. Quite often, the inconsistency of a draft law with the Constitution of Ukraine is highlighted by internal structural units of the Apparatus of the Verkhovna Rada of Ukraine, to which draft laws are mandatorily submitted for the preparation of opinions, namely the Main Scientific and Expert Department and the Main Legal Department (Article 103(2) of the Rules of Procedure of the Verkhovna Rada of Ukraine), as well as by the National Academy of Sciences of Ukraine, which is involved in conducting expert assessments of registered draft laws that are of a systemic

nature for specific branches of legislation and require scholarly examination, as determined by the relevant parliamentary committee at the stage of preparation for the first reading (Article 103(3) of the Rules of Procedure of the Verkhovna Rada of Ukraine) [17].

As law-making practice demonstrates, constitutional incompatibility does not necessarily prevent the discussion and advancement of a draft law through the procedures laid down in the Rules of Procedure of the Verkhovna Rada of Ukraine. There are numerous instances in which the legal positions of the Constitutional Court of Ukraine, as articulated in its judgments on matters that have a logical and substantive connection with the subject matter of the relevant draft law, are disregarded.

According to the methodological guidelines of the European Commission on the preparation of draft legal acts, known as the ‘Better Regulation Toolbox’ (July 2023 edition), a ‘threat-based approach’ is intended to eliminate the threat itself without a thorough risk assessment, where the risk is assumed to exist on the basis of general considerations, that is, the likelihood of adverse effects. At the same time, this approach is not equivalent, in terms of the methods of legal intervention applied to a given set of social relations, to a risk-based approach. The latter aims to control or limit the impact of a threat through risk management, which is acknowledged as inherently carrying a risk (Better Regulation Tool No. 14 ‘Risk Assessment and Risk Management’) [18, p. 103].

The application of threat-based approaches and risk-assessment-based approaches contributes to determining the degree of negative impact of a risk and the level of its acceptability in light of the scale of the threats generated. The legislative drafting techniques relied upon by the relevant services of the European Commission in the preparation of draft legal acts require the adoption of measures aimed at identifying the most significant risks and threats by types of impact, which are presented in a systematised manner in Section 4 of Better Regulation Tool No. 18, ‘Identifying Impacts’.

The total of 36 different types of impacts are identified, the obligation to assess which derives from a number of provisions of the Treaty on the Functioning of the European Union (Articles 8–14 TFEU). The ranking of impacts of different policy implementation options of the European Union on a given sphere of social relations is structured in such a way that a clear linkage is observed between a specific type of impact and the relevant Better Regulation tools to be applied in the analytical process, as well as with the

Sustainable Development Goals for the period up to 2030, the achievement of which legislative initiatives are intended to promote.

The variability of risks and threats capable of causing harm to the interests of the State and society, to legally protected rights, freedoms and interests of the individual and the citizen, as well as to the rights and legitimate interests of legal persons, depends on the completeness of the responses to control questions ('key questions', 'checklists'), which are not exhaustive. Consistent and structured responses to these control questions enable the drafter of a legal act to identify the presence of factors that form a system of risks and threats and to develop an algorithm of subsequent actions, allowing for the assessment of the degree of potential adverse impact and for the determination of measures aimed either at the full elimination of the threat or at permitting its existence within safe and controlled limits.

It is important to note that certain types of impacts have a cross-cutting nature and, in terms of their expected effects, may encompass issues the resolution of which requires the use of instruments provided under different Better Regulation tools. At the same time, the impact assessment process must, as a mandatory element, provide for reporting on the results of the screening of a legislative initiative in order to determine the extent to which such types of impacts as those on small and medium-sized enterprises, competitiveness, and fundamental rights have been taken into account. [18, p. 141].

It should be emphasised that fundamental rights enshrined in acts of EU primary law, first and foremost the Charter of Fundamental Rights of the European Union, as well as in a number of international legal instruments of the United Nations and the Council of Europe, constitute the basis for analytical work aimed at assessing the impact of proposed legislative initiatives on the state of legal regulation of a given set of social relations, insofar as such assessment contributes to the achievement of the Sustainable Development Goals, in particular Goal No. 16, 'Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels'. This goal is identified as one of the impact areas relevant to fundamental rights and, in conjunction with Target 16.3, 'Promote the rule of law at the national and international levels and ensure equal access to justice for all', [19], explains the foundational role of the findings obtained as a result of the impact analysis for recognising the integrity and completeness of the measures undertaken to assess the impact of the envisaged legal regulation.

In the list of control questions, the answers to which are intended to indicate the presence or absence of risks and threats to fundamental rights, a number of questions are set out across different chapters of the Charter of Fundamental Rights of the European Union [13]. In particular, under the chapter ‘Justice’, the expected impact and the degree of its compliance with the following provisions must be determined, namely: the right to an effective remedy and to a fair trial, the presumption of innocence, the principle of legality, the prohibition of retroactive application of criminal law, and the prohibition of being tried or punished twice for the same criminal offence (ne bis in idem) [18, p. 151]. Additionally, the preventive mechanism for assessing impacts on social relations within the category of fundamental rights is further elaborated within Better Regulation Tool No. 29 ‘Fundamental Rights, including the Promotion of Equality’ [18, pp. 244 – 250].

It can already be stated that the introduction into national law-making practice of such a stage of legislative drafting as the impact assessment of a draft normative legal act, as declared by the Law of Ukraine ‘On Law-Making Activity’ of 24 August 2023 No. 3354-IX, will require substantial improvement of the approach itself. In the text of the said Law, this approach lacks sufficient detail, while the instrumental framework for conducting impact assessments, including the definition of indicators to be expressed in the form of control questions (‘key questions’, ‘checklists’) correlated with the Sustainable Development Goals, EU law, and acts of international law, has not been properly established. In practice, Article 30 of the Law of Ukraine ‘On Law-Making Activity’ reflects the prevailing approach to the preparation of explanatory memoranda to draft laws, where it is often stated in a single sentence that there is no impact or only a potential minor impact on social relations, or, as is the case in the majority of instances, where no reference whatsoever is made to a specific type of expected impact. Impact assessment with regard to fundamental rights, which should be examined in the context of the completeness of compliance with and implementation of the principle of the rule of law as the foundation of the national legal order, pursuant to Article 8 of the Constitution of Ukraine of 28 June 1996 [20], is in practice not carried out by the drafter of a draft law. This situation is further reinforced by the inaction of the committee of the Verkhovna Rada of Ukraine responsible for constitutional law matters, which, in accordance with the Resolution of the Verkhovna Rada of Ukraine ‘On the List, Composition and Areas of Competence of the Committees of the Verkhovna Rada of Ukraine

of the Ninth Convocation' of 29 August 2019 No. 19-IX, is the Committee on Legal Policy.

It is precisely the activity of the committee of the Verkhovna Rada of Ukraine whose remit covers matters of constitutional law that is associated with the monitoring of draft laws for the purpose of identifying unconstitutional provisions (Articles 94 and 118 of the Rules of Procedure of the Verkhovna Rada of Ukraine) [17]. However, the activity of this committee is based on the principle of discretion, which provides for the preparation of a relevant opinion either on the committee's own initiative or at the request of the lead committee of the Verkhovna Rada of Ukraine. This leaves considerable scope for discretionary decision-making, which should instead be reflected in a regulatory design closer to the provisions of Article 19(2) of the Constitution of Ukraine, by establishing not a right, but a duty to conduct an assessment of draft laws for their compliance with the Constitution of Ukraine. The current model for organising the work of the parliamentary committee responsible for constitutional law matters and its involvement in legislative drafting, combined with the optional nature of scientific and legal expert opinions and the fact that the lead committee has a right, rather than an obligation, to take into account the comments expressed in such opinions (Articles 103(5), 117(2), and 118(6) of the Rules of Procedure of the Verkhovna Rada of Ukraine), collectively creates preconditions for the incorporation of unconstitutional normative legal acts into the legal system of Ukraine.

The approach applied by the European Commission to assessing the impact of proposed legislative initiatives on various spheres of social relations, based on a typology of impact factors, taking into account the variability of responses in the event that risks and threats are identified, and embedded in a systemic linkage with the fundamental values of the European Union, the Sustainable Development Goals, and acts of international law, with particular emphasis on the cross-cutting functional role of fundamental rights, should be incorporated into a modern methodology of legislative drafting. Such incorporation would contribute to enhancing the quality of legislation and ensuring its compliance with the Constitution of Ukraine.

The urgent need to implement the above-described approach may be demonstrated by reference to the introduction of a model of legal regulation that renders impossible, or ensures only partial, implementation of the provisions of the Constitution of Ukraine due to the failure or improper performance by authorised public authorities of their positive or negative

obligations, whether expressly or implicitly established, to regulate social relations on the basis of law. This gives rise to a phenomenon of legal reality which, in constitutional-law doctrine, is terminologically defined as ‘legislative omission’.

Without engaging, within the scope of this study, in a comprehensive analysis of the theoretical and practical aspects of legislative omission, which has been undertaken by the authors of this chapter in a separate scholarly work, it appears appropriate to emphasise that, according to the commonly accepted classification of legislative omissions, the most significant threats to the national legal order are posed by so-called ‘absolute’ legislative omissions, where the subjects of law-making fail to establish legal regulation that ought to have been enacted [21, p. 16].

As demonstrated by the practice of the Constitutional Court of Portugal, ‘absolute’ legislative omissions result not only from the failure to fulfil positive obligations, but also from the breach of negative obligations, namely the obligation to refrain from engaging in law-making activity in a manner that would render the implementation of constitutional provisions impossible. In particular, one example of the occurrence of a legislative omission recognised by the Constitutional Court of Portugal is the repeal of laws intended to give effect to constitutional norms without the introduction of legal regulation ensuring the implementation of a specific constitutional provision [21, p. 45].

In national law-making practice, an example can be identified in which the actions of the Parliament of Ukraine have created a situation whereby, as a result of the repeal of a number of laws of Ukraine, legal regulation of certain groups of social relations is currently absent, which runs counter to the provisions of the Constitution of Ukraine.

In particular, notwithstanding point 36 of Article 85 (1) of the Constitution of Ukraine, pursuant to which the powers of the Verkhovna Rada of Ukraine include the approval of the list of objects of state property that are not subject to privatisation and the determination of the legal framework for the expropriation of objects of private property, the Law of Ukraine ‘On the List of Objects of State Property Not Subject to Privatisation’ of 7 July 1999 No. 145-IX was repealed.

At the same time, the Constitutional Court of Ukraine adopts a rather cautious and restrained approach in assessing facts that may indicate the existence of a legislative omission. In particular, Ruling No. 6-up/2024 of 1 October 2024, closing the constitutional proceedings in the case initiated by

a constitutional petition of 51 Members of Parliament of Ukraine concerning the conformity with the Constitution of Ukraine (constitutionality) of the provisions of Section I and the second paragraph of subparagraph 1 of point 2 of Section II of the Law of Ukraine ‘On Declaring the Law of Ukraine ‘On the List of Objects of State Property Not Subject to Privatisation’ to Have Lost Its Force’ (hereinafter – Ruling No. 6-up/2024), demonstrated the Court’s reluctance to recognise situations of absence of legal regulation, where such regulation is envisaged by the Constitution of Ukraine, as manifestations of legislative omission.

This follows from the provision set out in the sixth paragraph of subparagraph 4.2 of paragraph 4 of Ruling No. 6-up/2024, according to which ‘the absence of a list of objects of state property not subject to privatisation approved by the legislator does not constitute a legislative omission and cannot be reviewed for conformity with the Constitution of Ukraine (constitutionality). This merely indicates that the legislator has not exercised its constitutional power as defined in point 36 of Article 85 (1) of the Constitution of Ukraine’ [22].

Other examples of breaches of the systemic linkage between acts of current legislation and the Constitution of Ukraine, which exacerbate legal uncertainty in society, have been addressed in other works by the authors of this chapter.

References

1. Дорожня карта з питань верховенства права. *Офіс Віце-прем’єр-міністра з питань європейської та євроатлантичної інтеграції*. Available at: https://eu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya_karta_z_pytan_verhovenstva_prava_2.pdf

2. Дорожня карта з питань реформи державного управління. *Офіс Віце-прем’єр-міністра з питань європейської та євроатлантичної інтеграції*. Available at: https://eu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya_karta_z_pytan_reformy_derzhavnogo_upravlinnya.pdf

3. Дорожня карта з питань функціонування демократичних інституцій. *Офіс Віце-прем’єр-міністра з питань європейської та євроатлантичної інтеграції*. Available at: https://eu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya-karta-z-pytan-funktsionuvannya-demokratychnyh-instytutstij.pdf

4. План заходів щодо захисту прав осіб, які належать до національних меншин (спільнот) України. *Офіс Віце-прем'єр-міністра з питань європейської та євроатлантичної інтеграції*. Available at: <https://eu-ua.kmu.gov.ua/wp-content/uploads/Plan-zahodiv-shhodo-zahystu-prav-osib-yaki-nalezhat-do-natsionalnyh-menshyn-spilnot-Ukrayiny.pdf>

5. Консолідовані версії Договору про Європейський Союз та Договору про функціонування Європейського Союзу. *Офіційний вебпортал Верховної Ради України*. Available at: https://zakon.rada.gov.ua/laws/show/994_b06#Text

6. Вступ до політичної системи Європейського Союзу / Науковий редактор Ярослав Шиманек. Warszawa: Wydawnictwo Akademii Wymiaru Sprawiedliwości, 2024. 258 с. Available at: https://aws.edu.pl/wp-content/uploads/2025/01/SZYMANEK-Wstep-do-systemu-politycznego-UE_UKR_www.pdf

7. Communication from the Commission to the Council and the European Parliament on Article 7 of the Treaty on European Union - Respect for and promotion of the values on which the Union is based. COM/2003/0606 final. *Eur-lex. Access to European Union Law*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2003:0606:FIN>

8. Communication from the Commission to the European Parliament and the Council a new EU framework to strengthen the rule of law. COM/2014/0158 final. *Eur-lex. Access to European Union Law*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52014DC0158>

9. Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget. *Eur-lex. Access to European Union Law*. Available at: <https://eur-lex.europa.eu/eli/reg/2020/2092/oj/eng#ntc4-LI2020433EN.01000101-E0004>

10. Комарова Т. та Лазовські А. Судова практика суду справедливості ЄС з питань верховенства права та її значення для України. Посібник. *Вища рада правосуддя*. Available at: https://hcj.gov.ua/sites/default/files/field/8830-0-8-24_posibnyk.pdf

11. Рішення Конституційного Суду України від 02.11.2004 № 15-рп/2004 у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень ст. 69 Кримінального кодексу України (справа про призначення судом

більш м'якого покарання). *Офіційний вебпортал Верховної Ради України*. Available at: <https://zakon.rada.gov.ua/laws/show/v015p710-04#Text>

12. Доповідь Венеційської комісії № 512/2009 «Верховенство права», яка схвалена на 86-му пленарному засіданні (Венеція, 25-26 березня 2011 року). Переклад на українську мову С. Головатого. *Право України*. 2011. № 10. С. 168–184.

13. Charter of Fundamental Rights of the European Union. *Eur-lex. Access to European Union Law*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT&qid=1725105390501>

14. Устименко В.А., Джабраїлов Р.А., Гудіма Т.С., Серебряк С.В. Принцип верховенства права як засіб утвердження фундаментальних цінностей: погляд крізь призму права ЄС та практики ЄСПЛ. *Вісник Національної академії правових наук України*. 2025. Том 32. Том 2. С. 87–114. <https://doi.org/10.31359/1993-0909-2025-32-2-87>

15. Теорія держави і права: підручник / [О.М. Бандурка, О.М. Головка, О.С. Передерій та ін.]; за заг. ред. д-ра юрид. наук, проф., акад. НАПрН України О.М. Бандурки; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 416 с.

16. Концепція забезпечення національної системи стійкості, затверджена Указом Президента України від 27.09.2021 № 479/2021. *Офіційний вебпортал Верховної Ради України*. Available at: <https://zakon.rada.gov.ua/laws/show/479/2021#Text>

17. Регламент Верховної Ради України, затверджений Законом України від 10.02.2010 № 1861-VI. *Офіційний вебпортал Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/1861-17#Text>

18. Better regulation toolbox (July 2023 edition). *European Commission website*. Available at: https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf

19. Transforming our world: the 2030 Agenda for Sustainable Development. United Nations. Available at: <https://sdgs.un.org/2030agenda>

20. The Constitution of Ukraine of 28 June 1996 No. 254k/96-VR. Official Web Portal of the Verkhovna Rada of Ukraine. Available at: <https://zakon.rada.gov.ua/laws/show/254k/96-vp?lang=en#Text>

21. General Report of the XIVth Congress of the Conference of European Constitutional Courts on Problems of Legislative Omission in

Constitutional Jurisprudence. Available at:
<https://www.venice.coe.int/files/Bulletin/SpecBull-legislative-omission-e.pdf>

22. Ухвала Великої Палати Конституційного Суду України від 01.10.2024 № 6-уп/2024 про закриття конституційного провадження у справі за конституційним поданням 51 народного депутата України щодо відповідності Конституції України (конституційності) приписів розділу I, абзацу другого підпункту 1 пункту 2 розділу II Закону України «Про визнання таким, що втратив чинність, Закону України «Про перелік об'єктів права державної власності, що не підлягають приватизації»». *Офіційний вебпортал Верховної Ради України*. Available at: <https://zakon.rada.gov.ua/laws/show/va06u710-24#Text>

Chapter 27
***The impact of European integration processes on the
development of the judiciary in Ukraine***
(L. Nikolenko)

Ukraine's European integration course is a determining factor not only for the state's foreign policy orientation but also for the profound transformation of its legal system, including the judiciary. Over the past two decades, the country has consistently sought to harmonize its national legislation with the norms of the European Union (EU) and the standards of the Council of Europe, which requires the implementation of the rule of law, the safeguarding of judicial independence, and the assurance of access to justice for all citizens. These efforts are critically important for Ukraine's further integration into the European legal community.

Historically, the Ukrainian judiciary has faced a number of structural challenges: insufficient judicial independence, low public trust in the judicial branch, corruption risks, and limited access to justice. The processes of European integration serve as a catalyst for systemic changes aimed at overcoming these problems and aligning the judicial system with modern European standards. At the core of these transformations lies the rule of law, which encompasses the legality and predictability of legal norms, fair and timely judicial proceedings, the independence and impartiality of the judiciary, and equal access to justice for all citizens.

Within the framework of the reforms undertaken, a comprehensive transformation of the judicial system can be observed, encompassing both the constitutional and legislative levels – such as the revision of procedural codes, the improvement of the judicial system, and the establishment of specialized institutions, including the High Anti-Corruption Court of Ukraine as well as the practical implementation of the standards of the

European Court of Human Rights (ECHR). The incorporation of ECHR case law into national practice contributes to the development of a unified approach to fair and effective justice.

The impact of European integration processes on Ukraine's judiciary is multidimensional. It encompasses both positive developments and achievements, as well as challenges related to judicial independence, staffing, the mitigation of corruption risks, and the adaptation of technological innovations. Examining these processes makes it possible to assess the current state of the judiciary in Ukraine, identify problematic aspects, and outline prospective directions for development that will enhance the efficiency, transparency, and public trust in the judicial branch in the context of European integration.

27.1. European integration standards of the rule of law and their implementation in Ukraine's judicial system

Ukraine's European integration course necessitates the systematic implementation of the principles of the rule of law, which are fundamental to the legal system of the European Union and the Council of Europe. The rule of law constitutes a complex normative and conceptual framework that ensures the supremacy of law over all legal subjects, the equality of citizens before the law, the fairness of judicial procedures, and the independence of the judiciary. In the context of European integration, these principles not only define the standards for the organisation and functioning of the judiciary but also serve as criteria for assessing the compliance of national legal systems with the requirements of the EU (*Acquis Communautaire*) and the case law of the European Court of Human Rights (ECHR).

In the national context, the concept of the rule of law is enshrined in the Constitution of Ukraine (Articles 8, 55, 124, 129), which proclaims the unity of the legal system, the supremacy of the Constitution, the independence of the judiciary, and the guarantees of the right to a fair trial [1]. The implementation of European standards requires the adaptation of these constitutional foundations to the demands of international law, including the provisions of the European Convention on Human Rights (hereinafter – the Convention) and the ECHR's case law, which establishes concrete criteria for

evaluating the fairness and effectiveness of judicial proceedings. In particular, Article 6 of the Convention, which guarantees the right to a fair trial, serves as a benchmark for the reform of national procedural legislation and judicial practice [2].

The standards of the rule of law encompass a range of interrelated aspects, each of which constitutes an integral element of the system of guarantees inherent to a democratic state governed by the rule of law. Legality, in this context, is understood as the mandatory observance by state authorities of norms adopted in accordance with prescribed procedures, as well as their conformity with the Constitution and the state's international obligations. However, legality cannot be confined to the mere formal application of the letter of the law; it presupposes the internal quality of normative acts, manifested in their clarity, predictability, coherence with universally recognised human rights principles, and their capacity to effectively regulate social relations [3]. Legality, therefore, is not limited to the mechanical compliance with procedures but also serves as a criterion of substantive justice within legal regulation, enabling the assessment of state decisions through the lens of their impact on individual rights and freedoms.

Legal certainty, as a component of the rule of law, presupposes the stability of legal regulation and the impossibility of arbitrary state interference in the rights and legitimate interests of individuals. In legal practice, this requires courts to develop coherent, predictable, and consistent case law that ensures equality among the participants in legal relations and contributes to strengthening public trust in the judiciary. The absence of legal certainty creates uncertainty in the application of laws, which in turn undermines the stability of the legal system and the effectiveness of judicial procedures. Thus, legal certainty functions not only as a technical standard of the rule of law but also as a guarantee of social predictability and legal security.

Proportionality is one of the fundamental standards of the rule of law, ensuring a balance between public interests and the protection of human rights and freedoms. In contemporary European legal understanding, this principle is designed to limit excessive or unjustified state interference in the realm of private rights. Its essence lies in the requirement that any restriction must pursue a legitimate aim, be necessary in a democratic society, and not exceed the measures sufficient to achieve the intended objective. In the case law of the European Court of Human Rights (ECHR), proportionality serves as a criterion for assessing the legitimacy of state interference. For instance,

in *Handyside v. the United Kingdom* (07.12.1976), the Court emphasised that freedom of expression may be restricted only to the extent necessary in a democratic society. In *Sunday Times v. the United Kingdom* (26.04.1979), the Court further clarified that any interference must correspond to a ‘pressing social need’. Thus, proportionality becomes a universal metric for evaluating the relationship between the intensity of the restriction and the importance of the pursued aim. In the national context, the principle of proportionality requires the identification of a legitimate aim for the restriction, verification of its necessity (including the absence of less restrictive alternatives), and an assessment of whether the degree of interference is commensurate with the weight of the public interest involved. Under martial law, this requirement becomes particularly relevant, as temporary limitations on rights and freedoms – imposed for reasons of security and defence – must remain proportionate, must not become arbitrary or excessive, and must retain an intrinsic connection to the aim of protection. From a scholarly and doctrinal perspective, proportionality embodies the synthesis of legality, justice, and legal certainty. It transforms the formal observance of the law into a just legal order in which the state, while restricting rights, simultaneously guarantees their effective protection. In this sense, proportionality functions not only as a technical legal instrument but also as a conceptual core of the rule of law, determining the quality of the legal system and its capacity to meet European integration standards.

The prohibition of arbitrariness by state authorities and courts is another key element of the rule of law. State activity cannot be based on discretionary or arbitrary decisions, as arbitrariness undermines the legitimacy of the legal order and creates a risk of violations of human rights. Every act of a state authority must have a clear legal basis, and judicial decisions must be reasoned, grounded in evidence and legal norms, take into account generally accepted international practice, and ensure a balance between the interests of the state and the rights of the individual. In its decision of 2 November 2004 (No. 15-rp/2004), the Constitutional Court of Ukraine emphasised that public power may not be exercised in a manner not prescribed by law, as this contradicts the principle of the rule of law, and that legality constitutes the fundamental criterion for assessing the permissibility of actions of public authorities [4].

Judicial independence and effective access to justice form the critical foundation for the realisation of these standards, as only genuinely independent courts are capable of providing effective protection of citizens’

rights and resisting any external pressure whether political or economic. These principles are particularly important in areas where judicial decisions may have a systemic impact on the economy and society, such as bankruptcy cases or corporate disputes, where a lack of judicial independence may lead to violations of creditors' rights and destabilisation of the financial environment. Effective access to justice becomes especially significant under martial law, when the state is compelled to introduce temporary restrictions to ensure national security and defence. At the same time, the rule of law requires that such restrictions do not result in a complete obstruction of judicial protection for individuals and legal entities. Access to justice under these conditions acquires a more complex nature: it must combine the capacity for rapid response to legal conflicts with the need to safeguard the security of participants and maintain the stability of judicial procedures. Under martial law, the priority becomes the protection of immediate and essential rights and freedoms, such as the right to life, health, property, and the performance of obligations. Courts are required to adapt their procedures by ensuring expedited case consideration, enabling remote submission of claims and applications, and utilising electronic platforms for hearings – measures that reduce risks for citizens and court personnel. At the same time, compliance with the principles of judicial independence and impartiality remains critically important. Any excessive limitation of justice in favour of state authorities, even in wartime, risks eroding trust in the legal system and creating conditions for arbitrariness. Special attention is given to ensuring access to justice for vulnerable groups, including internally displaced persons, persons affected by hostilities, and individuals with limited financial means. During this period, the state must ensure that temporary restrictions do not become disproportionate barriers to the exercise of procedural rights, the assurance of fairness, and the protection of property and personal interests. Effective access to justice during martial law thus becomes an indicator of the state's ability to reconcile security with the rule of law, demonstrating that even under crisis conditions the legal system remains capable of protecting rights and freedoms while maintaining a balance between the interests of the state and the individual. Therefore, in the context of martial law, effective access to justice is not limited to formal procedures; it emerges as a dynamic and adaptive mechanism that provides genuine protection of rights and freedoms, ensures fairness, and prevents arbitrariness, all while taking into account the specific nature of emergency conditions and the priorities of national security.

Equality in the application of legal norms presupposes that no individual or group of individuals may receive privileged or restricted access to justice on the basis of their social, economic, political, or any other status. Such equality prevents discrimination, promotes the fair protection of the rights of every participant in legal relations, and strengthens public trust in the legal system, which is a necessary condition for the stability of social institutions and the legitimacy of state authority. The primacy of human rights in the administration of justice serves as an imperative criterion for evaluating state activity, extending to all its branches the judicial, legislative, and executive. This means that any state acts, judicial decisions, or legislative initiatives must be assessed through the prism of their impact on individual rights and freedoms. In practical terms, the implementation of this principle requires that the Ukrainian judiciary move beyond the mere formal observance of procedures and ensure a conscious and proactive orientation toward the protection of fundamental human rights. This includes heightened attention to procedural fairness, access to justice, the proportionality of restrictions, and the prevention of arbitrary interpretation of legal norms. Moreover, this principle becomes particularly relevant under contemporary conditions in which the state faces crises or extraordinary circumstances. In such situations, the risk of restricting human rights increases significantly, and equality before the law becomes a criterion for assessing whether state measures comply with the standards of the rule of law. The judicial system must adapt its procedures to preserve fairness, ensure equal access to justice, and protect vulnerable groups of citizens, while not infringing upon fundamental human rights principles. Thus, equality before the law and the primacy of human rights function not only as normative standards but also as practical mechanisms for ensuring the fairness and legitimacy of state decisions. They constitute an indispensable precondition for Ukraine's full European integration, demonstrating the national legal system's ability to combine efficiency, stability, and the protection of individual rights even under the most challenging circumstances.

The process of implementing the standards of the rule of law involves a complex interaction of normative, institutional, and procedural mechanisms that ensure the effective realisation of these principles within the national legal system. One of the key aspects of this process is the constitutional-institutional level, which encompasses the systematic establishment and reform of judicial bodies, the development of the professional and ethical components of the judiciary, and the introduction of transparent and

accountable procedures for the functioning of judicial authority. A central task in this context is ensuring judicial independence a fundamental precondition for the rule of law that guarantees the impartiality of judicial decisions and protection from any external pressure, whether political or economic. An important component of the constitutional-institutional approach is the enhancement of transparency in the procedures for judicial appointment, disciplinary oversight, and performance evaluation, implemented through the activities of the High Council of Justice and the High Qualification Commission of Judges. These mechanisms not only formalise the processes of selection and oversight but also provide for public accountability in the formation of the judiciary, strengthen public trust in the judicial system, and promote the consolidation of legal culture based on legality and justice. It should be noted that the constitutional-institutional level of implementing the rule of law is not only structural but also strategic in nature. It ensures the harmonisation of the formal organisation of courts with the practical application of the law, creating an integrated system capable of meeting European standards of effective, transparent, and fair justice. At the same time, it establishes a balance between judicial autonomy and accountability for professional conduct, which is a key factor in ensuring the stability of the judicial system and the effective protection of citizens' rights and freedoms.

The legislative-procedural level of implementing the standards of the rule of law encompasses the systematic harmonisation of national procedural law with European legal benchmarks, which requires not only the adaptation of individual norms but also a rethinking of the very model of justice in light of the *acquis communautaire*. This involves the development of procedural mechanisms that ensure effective protection of individual rights, accessibility and timeliness of judicial procedures, as well as full compliance of legislation with the principles of predictability, stability, and proportionality of legal regulation. Particular attention should be paid to the quality of evidence, as it determines the effectiveness of procedural guarantees and the fairness of judicial proceedings. European standards emphasise that courts must not merely apply procedural norms formally but should also ensure conditions for the full and comprehensive establishment of the facts of a case. This requires the introduction of procedures that prevent manipulation of evidence, ensure its proper assessment, and promote uniformity of approaches in law enforcement.

At the same time, a key aspect is the legislative-drafting approach aimed at creating legal acts that meet the criteria of legal quality established in the

case law of the ECHR, namely: clarity, accessibility, foreseeability, and internal logical coherence. In this context, legislative drafting serves not merely as a technical activity but as a methodological tool for preventing legal uncertainty and conflicts of norms that may undermine public trust in the judicial system. The application of European standards to the law-making process requires legislators to consider not only national needs but also broader European trends in the development of law, which in turn enhances the stability and effectiveness of judicial protection [5]. Thus, the legislative-procedural level is decisive in the implementation of the standards of the rule of law, since it is through high-quality legislative drafting, effective evidentiary standards, and the harmonisation of procedural mechanisms with European benchmarks that the fundamental capacity of Ukraine's judicial system to ensure justice and reliable protection of rights in accordance with European values is formed.

The substantive-law level of implementing the standards of the rule of law encompasses the substantive content of legislation, its quality, and its capacity to ensure genuine protection of human rights and freedoms. A central element of this level is the principle of legal certainty, which requires legal norms to be formulated in a manner that is clear, foreseeable, and consistent with the existing legal system. Norms must not only regulate the behaviour of participants in legal relations but also prevent arbitrary interpretation or application. An important substantive-law standard is the principle of proportionality, which provides that any restriction of rights and freedoms must pursue a legitimate aim, be necessary in a democratic society, and remain within limits determined by that aim. Thus, legislation must contain built-in safeguards against excessive state interference in the private sphere. No less significant is the integration into national law of substantive standards derived from the case law of the ECHR. This primarily concerns the enshrining of guarantees of the right to property, freedom of entrepreneurial activity, the right to respect for private and family life, and adequate social protections. These provisions form the substantive-law core of the rule of law, oriented toward affirming human dignity as the highest value. A distinct importance is attached to the concept of good governance, which requires legislation to establish standards of good faith, transparency, and foreseeability of state actions in its relations with the individual. The substantive-law level of implementing the standards of the rule of law therefore entails not only the formal alignment of national norms with European requirements, but also a fundamental rethinking of the very content

of law as an instrument for protecting individuals from arbitrariness, ensuring a balance between personal and societal interests, and shaping a legal system capable of reflecting the values of the democratic European community.

The practical aspect of implementing the standards of the rule of law involves not only the formal consideration of international norms by national courts but also the systematic adaptation of judicial practice to the principles and precedents of the ECHR, including the active use of ECHR judgments as guidance for interpreting national legislation. This ensures the harmonisation of law enforcement and contributes to the unification of judicial practice throughout the country. Adaptation to international standards includes the analysis of specific judicial cases, the use of comparative law methods, and the integration of principles recognised within the European community into the daily work of the courts. An equally important element of the practical level is the development of institutions capable of providing effective mechanisms for the protection of human rights. This includes the establishment of specialised judicial chambers, the introduction of procedures for monitoring and evaluating the quality of judicial decisions, the use of modern technologies to enhance access to justice (electronic filing of documents, remote hearings), as well as the development of training and professional development systems for judges in the fields of international law and human rights. The practical aspect of implementation also involves active work at the level of judicial doctrine, whereby national courts develop coherent approaches to the application of legal norms based on international standards and the principles of the rule of law. Such an approach not only increases the effectiveness of judicial protection but also strengthens public trust in the legal system, ensures the predictability of judicial decisions, and prevents arbitrariness on the part of state authorities.

Thus, the practical level of implementing the standards of the rule of law entails the direct incorporation of European legal norms and principles into the everyday functioning of the judiciary, the establishment of effective institutional mechanisms for the protection of human rights, and the development of judicial practice that meets the high European standards of fairness, proportionality, and legal certainty.

Therefore, the implementation of European integration standards of the rule of law in Ukraine constitutes a comprehensive process that encompasses the constitutional, legislative, and practical dimensions of the functioning of the judiciary. It is aimed at ensuring judicial independence, enhancing the quality of justice, and integrating the Ukrainian judicial system into the

European legal space an essential prerequisite for the realisation of the state's strategic course toward European integration.

27.2. Harmonisation of Ukraine's procedural legislation with European standards

The harmonisation of Ukraine's procedural legislation with European standards is an integral component of the European integration process aimed at securing Ukraine's accession to the EU. This process entails the adaptation of national norms of commercial, civil, criminal, and administrative procedural law to the EU *acquis communautaire*, the recommendations of the Council of Europe, and the case law of the ECHR. According to the EU–Ukraine Association Agreement (2014), harmonisation must ensure the rule of law, the protection of fundamental rights and freedoms, and the effectiveness of judicial proceedings. In 2024–2025, this process gained particular momentum in the context of the screening of Ukrainian legislation for compliance with EU norms, which constitutes a key element of the accession negotiation process. Progress in harmonisation is reflected in the reports on the implementation of the Association Agreement, where the level of implementation in the field of justice and human rights reached 88% as of 2023–2024, with a specific emphasis on judicial reforms [6].

It should be emphasised that harmonisation does not consist in the literal transplantation of the *acquis communautaire* into Ukrainian law but rather involves the systemic integration of international legal standards into the national procedural framework while preserving national legal identity. Its purpose is not to produce a 'copy' of European models but to develop a procedural mechanism that simultaneously complies with international criteria of fair justice and takes into account the specific features of Ukraine's constitutional order, judicial organisation, and doctrinal traditions.

It is important to distinguish harmonisation from related categories, namely adaptation and unification. In EU law, harmonisation is understood in both a broad and a narrow sense. In the broad sense, it refers to the replacement of the national policies of the Member States with a single common Union policy in the relevant field; in the narrow sense, it denotes the substantive approximation of national legal rules to the standards established by the Union through the elimination of divergences in national legislation [7]. Furthermore, harmonisation and adaptation differ significantly in terms of the ability of the parties to influence each other's

legal order. In the case of the adaptation of third-country legislation to EU law, the process is strictly unilateral. Such states cannot influence the law-making mechanisms of the EU system, cannot amend EU legal norms, and cannot create a joint legal space of a united Europe together with the Member States. Thus, third states are merely incorporated into the already existing EU legal order [8]. The concept of ‘harmonisation’ refers to the process of aligning legislation with EU law that takes place within the EU and constitutes a statutory obligation exclusively of the Member States. Adaptation likewise describes the process of aligning legislation with EU law, but it typically occurs outside the EU and concerns third states seeking integration into the Union, as well as states that have already acquired membership but, while still in candidate status, did not complete this process [9]. In the latter case which applies to Ukraine such states must, for a certain period, simultaneously perform two types of activities: (1) ongoing (post-accession) harmonisation of their national legislation jointly with other Member States, and (2) the adaptation of their legislation to EU law with respect to those pre-accession obligations that were not fulfilled [10].

It should be emphasised that the adaptation of procedural legislation is a process of adjusting existing national norms to the requirements of European law. It has a more pragmatic and gradual character and often serves as the initial stage of harmonisation processes aimed at achieving minimum standards of compliance. Unification of legislation, by contrast, refers to the creation of uniform norms that operate identically across several legal systems (for example, within international conventions or integration frameworks). In the Ukrainian context, the unification of procedural legislation with EU law is limited in scope, as it does not entail a complete alignment of legal orders but rather their mutual compatibility.

Therefore, the harmonisation of Ukraine’s procedural legislation is a more complex and multidimensional phenomenon than adaptation or unification. It serves as an integrative formula for the development of national procedural law, combining the flexibility of adaptation with the systemic character of unification, and ensuring Ukraine’s balanced entry into the European legal space without losing its own legal identity.

The fundamental reference points of this process are the provisions of the 1950 European Convention on Human Rights, the 2000 Charter of Fundamental Rights of the European Union, as well as the case law of the ECHR and the Court of Justice of the European Union (CJEU). These instruments constitute the conceptual foundation of the European model of

justice, in which human rights are recognised not as a declarative value but as an operative criterion for evaluating the procedural system. European procedural standards are grounded in fundamental principles, foremost among which is the right to a fair trial (Article 6 ECHR), guaranteeing every individual the right to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. This principle encompasses a set of interrelated elements aimed at ensuring the overall fairness of the proceedings and applies to commercial, civil, and criminal cases, taking into account their specific characteristics. The elements of the right to a fair trial include the independence and impartiality of the court. Independence requires the judiciary to be free from external influence, while impartiality demands freedom from internal bias. Independence is assessed using criteria such as the method of appointment of judges, the duration of their tenure, guarantees against external pressure, and the availability of legal safeguards. Impartiality is divided into subjective impartiality (the absence of personal bias) and objective impartiality (the absence of circumstances that might give rise to legitimate doubts regarding impartiality). In the case law of the ECHR, for example, in *Findlay v. the United Kingdom* (1997) a violation was found due to the lack of independence of a military tribunal. For Ukraine, this issue is particularly relevant in the context of ongoing judicial reforms, where challenges include political influence on judicial appointments, as noted in the reports of the Venice Commission. As of 2024–2025, harmonisation requires strengthening the role of the High Council of Justice and the implementation of anti-corruption mechanisms in accordance with ECHR recommendations [11].

Another element of the right to a fair trial is the requirement that cases be examined within a reasonable time. The right to a hearing “within a reasonable time” begins from the moment charges are brought (in criminal cases) or a claim is filed (in commercial or civil cases) and ends with the final decision. The factors used to assess reasonableness include the complexity of the case, the conduct of the parties, the actions of state authorities, and the broader context (for example, martial law). The adversarial nature of proceedings is also part of the right to a fair trial and requires that the parties have the opportunity to present their arguments and evidence and to comment on the submissions of their opponent. This principle is closely linked to the right to effective defence and prohibits “secret” evidence or procedures. In criminal cases, it includes the accused’s right to examine witnesses (Article 6 § 3 (d)). A classic example is *Ruiz-Mateos v. Spain* (1993), where the lack of

adversarial proceedings led the Court to find the process unfair. In the Ukrainian context, harmonisation requires amendments to procedural codes to ensure full disclosure of evidence. As for equality of arms, this element ensures a balance of opportunities between the parties, including access to evidence, legal assistance, and resources. For Ukraine, where state authorities often possess greater resources, harmonisation requires strengthening free legal aid (Law of Ukraine ‘On Free Legal Aid’, 02.06.2011 No. 3460-VI). Additional elements of Article 6 include the publicity of proceedings (with exceptions for national security or morals), the right to a reasoned judgment, and specifically in criminal cases guarantees such as the presumption of innocence, the right to an interpreter, and the right to appeal. These principles serve as guiding benchmarks for reforming Ukrainian procedural legislation, particularly through amendments to the procedural codes. Harmonisation also takes into account the recommendations of the Venice Commission and the Council of Europe aimed at strengthening judicial independence and combating corruption, with a strong focus on the execution of ECHR judgments in Ukraine, where, as of 2025, challenges persist due to institutional weaknesses and the wartime context.

Effective legal protection, enshrined in Article 13 of the Convention, constitutes an autonomous right that imperatively guarantees every person whose Convention rights have been violated access to an effective remedy before a national authority. This guarantee applies irrespective of the status of the actors responsible for the violation and underscores the principle of subsidiarity of the Convention mechanism while preventing the protection of fundamental rights from becoming illusory. The ECHR emphasises that this principle is not subsidiary to the other provisions of the Convention but interacts organically with them, strengthening their implementation through the requirement that national legal systems create genuine mechanisms assessed according to the criteria of accessibility (absence of temporal, financial, or procedural barriers), effectiveness (the ability to prevent the continuation of a violation or to provide adequate redress, including compensation or restitution), practicality (applicability in everyday legal practice), and the independence of the competent authority (freedom from external pressure and assurance of impartiality). These elements form the foundation for the dynamic development of European standards of justice through the evolutionary interpretation of the Convention as a “living instrument” capable of adapting to contemporary challenges such as the digitalisation of justice or cross-border legal conflicts. In the context of

harmonising Ukraine's procedural legislation with European standards, Article 13 serves as a key benchmark for systemic reforms aimed at transforming remedies in civil, criminal, administrative, and commercial proceedings, with an emphasis on integrating the principles of the rule of law as reflected in the recommendations of the Venice Commission and the Council of Europe. Harmonisation involves not only the normative approximation to the *acquis communautaire* but also institutional changes, including the optimisation of the free legal aid system, the debureaucratisation of appeal procedures, and the development of flexible mechanisms that balance potential derogations from Convention obligations in emergencies with the inviolability of fundamental rights. These measures facilitate Ukraine's integration into the European legal space by strengthening institutional resilience, countering corruption risks, and enhancing the effectiveness of the judicial system amid contemporary geopolitical and social transformations.

The prohibition of discrimination, enshrined in Article 14 of the Convention and further elaborated in Protocol No. 12 to the Convention and in Articles 20–23 of the Charter of Fundamental Rights of the European Union, constitutes a fundamental principle of procedural law that directly affects the content and forms of exercising the right to a fair trial. Its essence lies in guaranteeing equal access to justice, equality of procedural opportunities, and impartial treatment of participants in judicial proceedings regardless of sex, race, ethnic origin, language, religion, political or other beliefs, social status, property status, or any other characteristic. Particularly significant is the assurance of gender equality in the administration of justice, as it represents both a concretisation of the principle of non-discrimination and a means of establishing substantive (factual) equality of the parties in procedural relations. The case law of the ECHR confirms that discriminatory manifestations in judicial proceedings constitute not only a violation of Article 14 of the Convention but also of Article 6, as they undermine the very essence of the right to a fair trial (*Abdu v. Bulgaria*, 2014; *Carvalho Pinto de Sousa Morais v. Portugal*, 2017). In these judgments, the Court emphasised the inadmissibility of gender stereotypes and biased judicial attitudes, which have the potential to undermine the legitimacy of justice and public trust in the judiciary. In the Ukrainian legal context, the implementation of the principle of non-discrimination and the guarantee of gender equality in procedural relations requires a comprehensive approach that includes: (1) the legislative enshrinement of specific mechanisms for protection against

gender discrimination in judicial proceedings; (2) the development of gender-sensitive judicial practice and adequate professional training for judges, lawyers, and prosecutors; and (3) a doctrinal rethinking of the principle of procedural equality not only as a formal but also as a substantive category that encompasses the real ability of the parties to defend their rights in court. Thus, the prohibition of discrimination and the guarantee of gender equality in judicial proceedings function not as isolated safeguards but as integral components of the principle of fair justice. Their effective implementation is a necessary condition for harmonising Ukraine's procedural legislation with European standards and an important indicator of the democratisation of Ukraine's judicial system.

The principle of proportionality and effectiveness in modern procedural law acquires a specific meaning through the growing emphasis on alternative methods of dispute resolution, which are regarded as a necessary complement to traditional judicial proceedings. These primarily include mediation, arbitration, negotiation procedures, as well as new forms of amicable settlement consistent with the European practice of 'friendly dispute resolution'. Such mechanisms allow for more flexible, faster, and economically efficient conflict resolution, reduce the burden on the judiciary, and ensure effective protection of the rights of the parties. In this context, the principle of proportionality requires the state to create legal and institutional conditions that enable the parties freely to choose the optimal form of protecting their rights, depending on the nature of the legal relationship and the intensity of the conflict. Moreover, the introduction of alternative dispute resolution mechanisms reflects a broader European trend of transforming justice from a predominantly punitive-repressive model to a consensual and agreement-based model, which focuses on restoring violated rights rather than solely on punishment or rigid judicial adjudication. This approach is particularly relevant to commercial procedure and bankruptcy proceedings, where the balance of interests is often achieved more effectively through negotiation and conciliation.

The harmonisation of Ukraine's procedural legislation with European standards cannot be uniform across all jurisdictions, since each type of judicial procedure has its own subject matter, value orientation, and functional purpose. Accordingly, European standards of fair trial are integrated differently into civil, commercial, criminal, and administrative proceedings, forming a complex system of mutually complementary models for protecting human rights and safeguarding public interests.

Civil procedure reflects the ‘classical’ implementation of the fair trial principles enshrined in Article 6 of the ECHR and developed in ECHR case law. The key benchmark here is ensuring access to justice, which requires the removal of excessive procedural barriers, maintaining a fair balance between the parties’ rights, and protecting vulnerable groups (children, low-income persons, persons with disabilities). European standards require the provision of equality of arms, clear regulation of time limits, and guarantees for the enforcement of judicial decisions. Particular attention is given to the development of mediation and arbitration, which constitute an important component of the principle of proportionality and help optimise dispute resolution outside an overburdened court system.

Commercial (economic) procedure is distinguished by its focus on ensuring the stability of business transactions and economic security. Here, harmonisation is based on the incorporation of the *acquis communautaire* in the fields of economic law and competition, including transparency in insolvency procedures, the effectiveness of corporate dispute resolution, and the protection of the rights of legal entities and entrepreneurs. Unlike civil proceedings, where the key element is the individual’s access to justice, commercial justice prioritises balancing the interests of business actors and investors. A special role is played by the institute of preventive restructuring, which requires Ukraine to undertake substantial modernisation of its national bankruptcy procedures. Commercial procedure is increasingly oriented toward integrating arbitration and conciliation mechanisms as tools for reducing transaction costs and enhancing the efficiency of justice.

Harmonisation in the criminal sphere is particularly sensitive, as it concerns the protection of fundamental human rights and freedoms from potential state arbitrariness. The ECHR has developed a set of guarantees that include the presumption of innocence, the right to defence from the moment of arrest, the right not to incriminate oneself, the prohibition of torture and ill-treatment, and the right to a fair trial within a reasonable time. For Ukraine, it is critically important to ensure the effectiveness of pre-trial investigations, prevent abuses of preventive measures, and expand the use of plea agreements and restorative justice, which reflect the humanistic transformation of criminal procedure. The balance between the rights of the accused and the victim remains a challenge, which the ECHR evaluates through the lens of proportionality of interference and the fairness of the procedure.

Administrative justice embodies the standard of effective control over public authority. Its harmonisation with European principles is oriented toward the realisation of the rule of law and the guarantee of the right to an effective remedy (Article 13 of the Convention). The Ukrainian model of administrative justice requires alignment with European practice in the areas of migration, tax, and electoral law, where the issues of timeliness, impartiality, and the effectiveness of judicial oversight are of decisive importance. A distinctive feature of administrative proceedings is their public-law nature, which demands clear regulation of procedural safeguards against abuses of power, including the right to judicial review of discretionary decisions by state authorities.

Therefore, the harmonisation of Ukraine's procedural legislation is not merely the 'implementation' of the *acquis communautaire* but rather a systemic transformation of the national procedural doctrine that takes into account the differences between jurisdictions. Civil procedure emphasises access to justice and equality of arms; commercial procedure focuses on economic stability and efficiency; criminal procedure centres on the protection of fundamental rights from state arbitrariness; and administrative procedure ensures control over public authority and protects individuals from abuses of power. European standards do not unify judicial proceedings but instead establish a shared axiological framework within which Ukraine shapes its own model of justice.

Based on the above, it can be stated that European integration processes manifest themselves not only in the normative harmonisation of Ukraine's procedural legislation with the *acquis communautaire* and the standards of the Council of Europe, but also in the profound methodological transformation of the national system of justice. They shape a new axiological paradigm of adjudication in which the principles of the rule of law, the protection of human rights, the efficiency of justice, and public trust in the judiciary as an institution of a democratic state become paramount.

The methodological significance of European standards lies in the fact that they establish universal criteria for assessing the fairness of judicial proceedings: access to justice, the independence and impartiality of the court, reasonable time limits, equality of arms, and the effectiveness of remedies. These standards are not only incorporated into national codes but also serve as instruments for the doctrinal rethinking of the judiciary's role within the separation of powers and in law enforcement. Thus, the impact of European integration processes on the development of Ukraine's judicial system is

complex and systemic in nature. European standards of justice serve as a methodological benchmark for the modernisation of the judiciary, enabling the assessment not only of the formal conformity of legal norms but also of the actual level of fairness and effectiveness of judicial procedures. In this sense, European integration is not an end in itself but sets the strategic direction for the evolution of Ukrainian justice towards the establishment of a stable, transparent, and fair judicial mechanism capable of safeguarding rights and freedoms even under conditions of societal crisis and transformation.

References

1. Принцип верховенства права: проблеми теорії та практики: у двох книгах, за заг. ред. Ю. С. Шемшученка; [ред. кол.: Ю. С. Шемшученко (голова)]. Книга друга: Принцип верховенства права у діяльності держави та в адміністративному праві / відп. ред. В. Б. Авер'янов. К.: Конус-Ю, 2008. 314 с.
2. Конвенція про захист прав людини і основоположних свобод: ратифіковано Законом України від 17 липня 1997 р. № 475/97. Офіційний сайт Верховна Рада України. Законодавство України. Available at: https://zakon.rada.gov.ua/laws/show/995_004#Text
3. Ніколенко, Л. М. (2025). Верховенство права як універсальний принцип забезпечення прав людини в сучасних умовах. Південноукраїнський правничий часопис. № 2. С. 14–18. <https://doi.org/10.32850/sulj.2025.2.3>
4. Швалюк, Д. Ю. (2025). Конституційний Суд України у забезпеченні верховенства права, як напрям функціонування в умовах євроінтеграції. Актуальні проблеми судового права : матеріали Х міжнар. наук.-практ. конф. / відп. ред. Л. М. Москвич. Харків: Право. С. 334–338.
5. Устименко, В.А. (2025). Адаптація національного законодавства до права Європейського Союзу: основи, критерії, виміри стійкості: Монографія; НАН України, ДУ «ІЕПД імені В.К. Мамутова НАН України». К.: Академперіодика. 452 с. Available at: <https://hozpravoreposit.kyiv.ua/handle/765432198/256>
6. Звіт про виконання угоди про асоціацію між Україною та Європейським союзом за 2023 рік. Available at: <https://eu->

ua.kmu.gov.ua/wp-content/uploads/Zvit-pro-vykonannya-Ugody-pro-asotsiatsiyu-mizh-Ukrayinoyu-ta-YEvropejskym-Soyuzom-za-2023-rik.pdf

7. Schweitzer, M. (1996). *Europarecht: das Recht der Europäischen Union, das Recht der Europäischen Gemeinschaften (EGKS, EG, EAG) mit Schwerpunkt EG*. Neuwied, Kriftel, Berlin: Luchterhand,. 631 s.

8. Яковюк, І. В. (2012). Адаптація законодавства України до законодавства Європейського Союзу: проблеми теорії і практики. *Європейський Союз і Україна: особливості взаємовідносин на сучасному етапі*; Національна академія прав. наук України; НДІ держ. буд-ва та місц. самоврядування. Харків: Оберіг. Розд. 1. С. 5–47. Available at: <https://dspace.nlu.edu.ua/jspui/handle/123456789/2191>

9. Пікуля, Т. О. (2024). Гармонізація законодавства в процесі переговорів про вступ України до Європейського Союзу. *Юридичний науковий електронний журнал*. № 8. С. 474–476. <https://doi.org/10.32782/2524-0374/2024-8/112>

10. Сокур, Т. А. (2023). Гармонізація та адаптація як інструменти правової інтеграції при взаємодії правових систем держав-членів з правопорядком ЄС і правовими системами країн – кандидатів. *Всеукраїнська науково-практична конференція. Класичний приватний університет*. С. 93–96. Available at: <http://catalog.liha-pres.eu/index.php/liha-pres/catalog/view/220/5209/11658-1>

11. Guide on article 6. Right to a fair trial (criminal limb). European Court of Human Rights. 2014. Available at: <https://rm.coe.int/1680304c4e>

Chapter 28
***The role of Ukraine in the transformation of the European
security order: from partnership to full membership***
(Ia. Petrunenko)

The full-scale aggression of the Russian Federation against Ukraine, which began in 2014, became a watershed moment in European security. It proved to be the greatest challenge to international and European security systems since World War II. This war effectively destroyed the illusions of ‘eternal peace’ in Europe that prevailed after the end of the Cold War. Security institutions created more than seven decades ago have demonstrated their inability to respond effectively to open armed aggression by a major power. Moscow is cynically attempting to reshape the existing European security order to suit its interests, in gross violation of international law. However, the consolidated response of Western countries to Russian aggression and Ukraine’s resilience have given rise to a large-scale transformation of the European security order.

The full-scale invasion of Ukraine by the Russian Federation in February 2022 finally put an end to the era of European security as a cooperative project based on the principles of the 1975 Helsinki Final Act and subsequent agreements between NATO, the OSCE and the Russian Federation. The old security order effectively collapsed, and there was a need to rethink and rebuild Europe’s security architecture in the context of continued Russian hostility [1]. Lincoln Gardner, researching the role of the OSCE in European security, aptly noted that by the beginning of 2025, after almost three years of war, ‘the rules-based order that once governed security on the European continent lies in ruins’ [2]. No international organisation or security mechanism – neither the UN, nor the OSCE, nor even NATO or the EU – was able to prevent Russia’s

aggression against Ukraine [2]. This war has highlighted the limitations of old institutions and principles and has become a catalyst for profound transformations in the European security order.

European countries, recognising the new reality, have significantly strengthened their defence capabilities. Many countries have increased their defence spending to levels unseen in previous decades. NATO has returned to the priority of collective defence: the alliance has significantly strengthened its eastern flank, deployed additional combat groups in Eastern Europe, and recognised Russia as the most direct threat to security in its new 2022 Strategic Concept. Due to Russia's aggression, Finland and Sweden, which had previously been neutral, made historic decisions to join NATO, a direct consequence of the Russian-Ukrainian war. At the same time, the EU, which has traditionally focused on 'soft' security instruments, has taken unprecedented steps to support Ukraine: for the first time in its history, the EU is financing the supply of lethal weapons to a country that is a victim of aggression (through the European Peace Fund), has deployed the EUMAM Ukraine (European Union Military Assistance Mission for Ukraine) to train Ukrainian military personnel, and has imposed the most extensive sanctions against the aggressor country. The war has also accelerated European integration processes: Ukraine applied for EU membership shortly after the invasion began and was granted candidate status in June 2022, and at the end of 2023, a decision was made to start accession negotiations. Also in September 2022, Ukraine applied for accelerated accession to NATO, underscoring a radical shift in its foreign policy course – from non-aligned partnership to seeking full membership in both leading Western alliances.

Thus, our country has come to play a key role in the transformation of the European security order. From a country that until recently was seen as a buffer 'grey zone' between NATO, the EU and Russia's sphere of influence, Ukraine is becoming an active player whose actions are changing the continent's security

architecture. Since the beginning of Russian aggression in 2014, Ukraine has gradually integrated into the Euro-Atlantic security space as an important partner, and after 2022 – as an outpost of collective security in Europe. Ukraine's further path 'from partnership to full membership' in Western security structures is no longer seen as a distant prospect, but is considered one of the decisive factors in the future European security order. The main dimensions of this transformation are analysed below: Ukraine's bilateral security agreements with leading democracies (as an interim security guarantee mechanism), the prospects for Ukraine's accession to NATO and the EU, Ukraine's direct influence on the formation of a new European security system, as well as the results and strategic conclusions regarding its role in these processes.

28.1. European security order until 2022: structure, principles, limitations

Until 2022, Europe's security architecture was based on several interrelated levels and organisations. The cornerstone of collective defence remained the North Atlantic Treaty Organisation (NATO), a military-political alliance of democratic states. Non-NATO countries were involved in security cooperation through partnership programmes. Ukraine, in particular, was the first of the post-Soviet countries to join NATO's Partnership for Peace programme [3] in 1994, and in 1997 signed the Charter on a Distinctive Partnership, which established the Ukraine-NATO Commission to deepen cooperation. At the same time, Ukraine had secured its non-aligned status and balanced between cooperation with NATO and restrictions imposed by the desire not to provoke Russia. Although it was declared at the 2008 NATO summit in Bucharest that Ukraine would «become a member» of the Alliance, the practical implementation of this decision was postponed indefinitely under pressure from geopolitical circumstances.

The EU, in turn, was primarily engaged in 'soft' security before the war – supporting stability through enlargement, neighbourhood and multilateral initiatives. The Eastern Partnership initiative (since 2009), designed to bring six Eastern European neighbours closer to the EU, was important for Ukraine. However, as the experts at the Razumkov Centre rightly pointed out, the

security potential of this initiative was limited: there are frozen conflicts in five of the six Eastern Partnership countries, and when war broke out between two of them – Armenia and Azerbaijan – in 2020, the EU effectively remained on the sidelines, while Russia and Turkey joined the settlement process [4]. This demonstrated that until 2022, the EU had no effective instruments to guarantee the military security of its eastern partners, limiting itself to diplomacy, sanctions and support for reforms.

The Organisation for Security and Cooperation in Europe (OSCE), which brought together almost all countries of the Euro-Atlantic and post-Soviet space, including Russia and Ukraine, played a major role in maintaining pan-European security. The principles of indivisible security, sovereign equality of states, non-interference and peaceful settlement of disputes, enshrined in the 1975 Helsinki Final Act [5] and the 1990 Paris Charter for a New Europe [6], were intended to serve as the moral and legal basis for the European security order. However, in practice, these principles have been repeatedly violated, particularly by the Russian Federation (the 1992 conflict in Transnistria, the 2008 war in Georgia, and the 2014 annexation of Crimea). The OSCE proved unable to stop the aggressive actions: its consensus decision-making mechanism, which was considered an achievement, became a major obstacle in crisis situations. When Russia launched a large-scale invasion in February 2022, no security structure – neither the UN, nor the OSCE, nor NATO, nor the EU – was able to prevent it. This highlighted the flaws in the old order, in particular the lack of effective security guarantees for countries that were not members of NATO. The experience of Ukraine is telling: having renounced its nuclear arsenal in the 1990s in exchange for security guarantees under the 1994 Budapest Memorandum, Ukraine subsequently saw that these guarantees did not work – neither in 2014 nor in 2022.

28.2. Full-scale invasion by the Russian Federation: a challenge to European security

The political and legal consequences of Russia's attack on Ukraine in February 2022 proved devastating for the nuclear non-proliferation regime: as the Ukrainian Foreign Ministry officially stated, Russia's violation of its obligations under the Budapest Memorandum created 'a dangerous precedent that undermined confidence in the very idea of nuclear disarmament' [7]. Consequently, countries that had once counted on international guarantees of

their security in exchange for renouncing weapons of mass destruction received a negative signal. The UN system also proved paralysed – Russia, as a permanent member of the UN Security Council, blocked any decisions that could stop its aggression.

As of May 2025, Russia maintains its permanent representation to the OSCE in Vienna. Its delegation participates in meetings of the Permanent Council and the Forum for Security Cooperation (FSC), where it actively promotes its own narratives and blocks decisions that contradict its interests (in 2023, together with Belarus, it blocked Estonia's appointment as chair of the OSCE). Russian parliamentarians do not participate in the work of the OSCE Parliamentary Assembly, but individual contacts between Russian representatives and members of the Assembly still take place. For example, in April 2025, the President of the OSCE Parliamentary Assembly, Pia Kauma, met with Russian Senator Konstantin Kosachev, which drew criticism from the Finnish government. In December 2024, Russian Foreign Minister Sergey Lavrov attended an OSCE meeting in Malta, his first trip to an EU country since the start of the war. There is currently no evidence that Russian citizens hold senior positions in other OSCE institutions, such as the Office for Democratic Institutions and Human Rights (ODIHR), the OSCE Representative on Freedom of the Media, or the High Commissioner on National Minorities, due to restrictions on Russia's participation in the organisation's activities because of its aggressive policies.

NATO faced an unprecedented situation of a major power waging war against a partner country that was not covered by Article 5 of the Washington Treaty on collective defence. However, the alliance had to respond to a direct threat to European security. First, plans to defend NATO's eastern flank were activated and the military presence of allies in the Baltic states, Poland, Romania, Slovakia and Hungary were sharply increased. Second, NATO members began large-scale arms deliveries to Ukraine to stop Russia's advance. Containing Russia became a top priority: by mid-2022, the previously neutral Finland and Sweden had renounced their non-aligned status and applied for NATO membership [1]. Germany announced a historic shift in security policy ('Zeitenwende'), increasing defence spending, while most NATO allies rapidly increased their military budgets [1]. By 2024, 22 of the 30 European NATO members had reached the target level of 2% of GDP for defence spending (in 2014, there were only two) [1]. Thus, it is clear that Russia's aggression prompted rapid militarisation and consolidation of NATO.

Ukraine's strategic status has also undergone a radical change. With the start of full-scale war, our country has finally made a civilisational choice in favour of the West. On 30 September 2022, Ukraine officially applied for accelerated accession to NATO [8]. A little earlier, on 23 June 2022, the European Council granted Ukraine the status of a candidate for EU membership [9]. Since then, accession to NATO and the EU has become Ukraine's officially recognised goal for the near future, and Ukraine itself has increasingly been viewed in international discourse as an integral part of the Western community.

However, the complete inability of the UN and the OSCE to respond adequately to the gross, open armed violation of international law by a permanent member of the UN Security Council (the Russian Federation) became a turning point in the global political and security system. In practice, the OSCE found itself blocked from within due to the principle of consensus, which allowed Russia to systematically block decisions, including personnel appointments and the extension of mission mandates [10]. During 2022-2025, Russia continued to be a member of the OSCE, exercising its rights but completely disregarding its obligations, while preventing the implementation of any new OSCE projects on its territory and sabotaging the organisation's activities in other countries [11].

The position of the UN was even more symptomatic. Despite massive war crimes, missile attacks on civilian infrastructure, and the use of force against a sovereign state, Russia remained unpunished within the UN Security Council, having the right to veto all decisions concerning its aggression [12]. In response, leading democratic countries, primarily G7 members, as well as Central and Eastern European countries, focused their efforts on creating flexible coalitions and functional security formats outside the framework of the UN and OSCE. The most striking example was the formation of a system of bilateral security agreements with Ukraine, which were launched in the development of the G7 Joint Declaration on Security Guarantees (Vilnius, July 2023) and covered more than 30 countries by the beginning of 2025. Although these security agreements are not full guarantees in the spirit of Article 5 of the Washington Treaty, they have de facto created a new network of commitments and long-term support for Ukraine's security sector, including military, cyber, intelligence and economic components [13].

In addition, it was under the pressure of military reality that such formats of cooperation as the Ukraine-NATO Council, the European Peace Fund

(EPF), the EUMAM Ukraine military assistance mission, and regular contact groups on defence issues (e.g., in the Ramstein format) were activated. The emergence of such structures indicates the gradual formation of a new multi-level security architecture in Europe, based on practical partnership and the ability to respond quickly, rather than on the universal but paralysed mechanisms of the post-bipolar period.

The processes that were launched in 2022 turned into a systemic restructuring of the European security landscape by the end of 2024 and early 2025. Ukraine found itself at the centre of this transformation, not only as the object of international support, but also as a full-fledged factor in the new balance of power, an initiator of strategic partnerships and a bearer of collective security values. Our country has demonstrated not only its capacity for sustained defence, but also its ability to institutionally rebuild itself and reform the security and defence sector, even in wartime.

The profound shock caused by Russian aggression has effectively delegitimised some of the existing international security institutions in their current form. At the same time, it has created a powerful impetus for the formation of a new generation of security mechanisms – functional, adaptive, based on trust and common interests. Ukraine is not only a beneficiary in this process, but also a catalyst; it is precisely through its experience and resistance that the future of European security is being shaped.

28.3. Ukraine as an active actor in European security

Full-scale war has transformed Ukraine from an object of decision-making by major powers into a subject that directly influences the security of the entire European continent. From the first days of the aggression, the Ukrainian state and society have demonstrated extraordinary resilience and defensive capabilities, earning the respect and support of the democratic world. The Armed Forces of Ukraine have effectively become the ‘shield of Europe’, holding back the Russian invasion on the eastern borders. As the then Commander-in-Chief of the Armed Forces of Ukraine, Colonel-General Ruslan Khomchak, noted in his official greeting to NATO on the anniversary of the alliance’s creation in 2021, ‘in recent years, the Ukrainian army has become a real shield of Europe’ [14], defending civilisational values from Russian aggression. In 2022-2023, this metaphor took on a literal meaning – the Ukrainian military is holding back the greatest military force threatening

all of democratic Europe, acting as the first line of defence of the common Euro-Atlantic space.

Today, Ukraine is an active participant in the European security system on several levels. Firstly, the Ukrainian army is rapidly integrating into NATO military standards, equipment and practices. The Armed Forces of Ukraine are adopting the advanced experience of Western armies in combat operations, receiving the most modern weapons and equipment from allies, and mastering their use in an extremely short time. In fact, the Ukrainian army is becoming the most combat-ready force in Europe and is achieving operational compatibility with the armies of NATO countries even before formally joining the alliance. Western partners, in turn, are providing Ukraine with an unprecedented amount of intelligence and information, significantly increasing the effectiveness of our country's defence. According to American media reports, the United States is sharing intelligence with Ukraine in real time; in particular, it was reported that it was the intelligence provided by the US that helped Ukraine successfully strike the flagship of the Russian Black Sea Fleet, the cruiser «Moskva», in April 2022 and neutralise a number of Russian generals on the front line [15]. This level of military-intelligence cooperation makes Ukraine a de facto part of the West's common defence space.

Secondly, Ukraine has become an initiator and active participant in new security formats and coalitions. In particular, in April 2022, the so-called Ramstein Contact Group was created – a coalition of more than 50 states led by the United States, which holds regular meetings of defence ministers and coordinates the provision of military assistance to Ukraine. Specialised 'capability coalitions' are also being formed within the framework of Ramstein, such as a tank coalition (to transfer Leopard 2 tanks to Ukraine), an aviation coalition (to train pilots and prepare for the transfer of F-16 fighter jets), an air defence coalition, and so on. Such a network of specialised agreements significantly strengthens the ability to respond collectively to aggression and is a new phenomenon in European security practice.

Thirdly, Ukraine is undergoing deep diplomatic integration into the Western security space. The Ukrainian leadership is constantly involved in consultations with NATO and EU leaders and participates in summits and meetings at the highest level. In 2023, a new institution was created – the Ukraine-NATO Council, where Ukraine and the alliance countries interact as equal participants, which was another step from the 'NATO-partner' relationship to the practical involvement of Ukraine in the security decision-

making process. In addition, Ukraine is synchronising its foreign and security policy with the EU: it is joining all EU sanctions packages against Russia, implementing European export control regulations, and actively cooperating in energy security and cyber defence. Ukrainian intelligence, counterintelligence and law enforcement agencies maintain close contacts with their Western counterparts, which allows them to more effectively counter common threats such as terrorism, cyberattacks, Russian intelligence and sabotage activities, etc.

Thus, in the midst of war, Ukraine ceased to be a ‘passive consumer of security’ and became an actor making a significant contribution to the collective security of Europe. The Ukrainian army, intelligence services and diplomacy work closely with the relevant NATO and EU structures, effectively acting as an ‘outpost’ of the democratic world in Eastern Europe. This radically changes the balance of power and the principles of European security, paving the way for Ukraine to become an integral part of the Euro-Atlantic security space in the future.

28.4. Bilateral security agreements (G7 countries, Great Britain, France, etc.)

Against the backdrop of open warfare against Ukraine and the postponement of the issue of its accession to NATO, Kyiv sought alternative mechanisms to ensure security. After the bitter experience of the 1994 Budapest Memorandum, which failed to protect Ukraine from aggression, the need for more effective agreements became apparent. In 2022–2023, various models were considered in expert circles: from Ukraine’s immediate accession to NATO (which would mean the automatic application of collective defence in the event of a new Russian attack) to ‘intermediate’ security guarantees from a group of leading states or the so-called ‘Israeli model’, under which Ukraine would remain outside NATO but would receive large-scale military assistance to independently deter Russia. As a result, Western capitals leaned towards an intermediate option: providing Ukraine with assurances of long-term support in the form of bilateral agreements with key allies, which would remain in force until Ukraine became a full member of the alliance.

An important step was the adoption in July 2023 of the G7 Joint Declaration on Support for Ukraine. On the sidelines of the NATO summit in Vilnius, the G7 countries (the United States, the United Kingdom, Germany,

France, Italy, Canada, and Japan) collectively declared the principles of long-term security commitments to Ukraine [16]. This document defined the framework within which each donor country would conclude specific bilateral agreements with Ukraine on security support. The G7 declaration specifically states the readiness to immediately begin consultations with Ukraine in the event of new aggression in order to determine the necessary response measures; the parties confirmed their intention to provide ‘rapid and sustained’ defence assistance to Ukraine – from modern military equipment to intelligence, as well as assistance in strengthening economic stability and implementing reforms that bring Ukraine closer to EU and NATO membership. At the same time, the G7 countries explicitly emphasised that these commitments are not analogous to Article 5 of the Washington Treaty, i.e. they do not provide for automatic military intervention on Ukraine’s side. In fact, these are political guarantees of long-term support, designed to strengthen Ukraine’s ability to defend itself and deter the aggressor.

In accordance with the G7 declaration, Ukraine is actively concluding bilateral security agreements with individual countries during the second half of 2023 and in 2024. The first such agreement was signed by the United Kingdom – on 12 January 2024, a ten-year Ukrainian-British Agreement on Cooperation in the Field of Security was concluded [17]. This document was the first practical result of the agreements reached in Vilnius. As expected, other key allies joined the process: as of early 2024, Ukraine was negotiating similar agreements with more than 30 countries. In total, 32 countries have already joined the G7 Joint Declaration, demonstrating broad international support for the format of long-term security guarantees for Ukraine. By mid-2024, Ukraine had signed bilateral security cooperation agreements with all G7 countries, as well as with a number of other partners in Europe (including Denmark, the Netherlands, Iceland, Norway, Spain, Portugal, Finland, Sweden, Latvia, and Belgium). Each agreement has its own specific features, but in general they are based on common principles and commitments.

Typical areas of cooperation enshrined in such agreements include: the supply of modern weapons and military equipment to the Armed Forces of Ukraine, the exchange of intelligence, the conduct of training and exercises for Ukrainian military personnel, support for the development of Ukraine’s defence industry, strengthening cyber security and countering hybrid threats, etc. For example, the United Kingdom has committed to helping strengthen Ukraine’s naval capabilities, Poland to developing the capabilities of its armoured forces, Lithuania to assisting in mine clearance activities, Japan to

cooperating in the field of cybersecurity and IT, and Spain to strengthening air defence, etc. The agreements are long-term (usually for a period of 10 years) and are intended to signal to Russia the West's long-term commitment to supporting Ukraine. At the same time, in most cases, the specific amounts of aid are fixed for the short term (1–3 years) and are subject to review depending on how the situation develops. For example, the aforementioned agreement with the United Kingdom specifies London's commitment to provide the current level of military assistance to Ukraine during the financial year, while the continuation and expansion of support will depend on individual political decisions by the government.

These bilateral agreements are extremely important for Ukraine, given the difficulties in obtaining immediate, legally binding guarantees of collective defence. The Ukrainian leadership sees them as an intermediate step on the path to NATO membership. Indeed, despite political support for Ukraine from its allies, there remains some uncertainty about the timing and conditions of its accession to the alliance, so bilateral security agreements are currently the only formalised instrument of long-term Western commitments to Ukraine. At the same time, such agreements do not require ratification by foreign parliaments and are political in nature, so their success will depend primarily on the political will and determination of future governments of these countries to fulfil their commitments. The existence of an extensive network of bilateral security agreements already integrates Ukraine into a common security space with Western countries. This also creates the basis for a new model of European security, which includes Ukraine as an integral part, strengthens its defence capabilities and brings it closer to full participation in allied structures. Thus, bilateral security agreements have become a flexible tool that combines political support and practical military assistance to Ukraine, while paving the way for its future accession to NATO.

28.5. Prospects for full membership in NATO and the EU

As mentioned above, the full-scale war has significantly accelerated Ukraine's Euro-Atlantic integration and made the issue of its membership in NATO and the EU one of the key items on the European political agenda. In 2022–2024, our country has already made unprecedented progress towards joining both organisations, but difficult tasks remain ahead – political, legal and military-security ones. It is already clear that the future security architecture of Europe will largely depend on whether Ukraine becomes a full

member of the Euro-Atlantic community. Accordingly, both Ukraine and Western institutions themselves must clearly define the further course of Ukraine's membership in NATO and the EU. At the same time, the timeframe for this process will largely be determined by the course of the war and the post-war security configuration in Europe [18].

NATO. Back at the Bucharest Summit in 2008, it was declared that Ukraine would eventually become a member of NATO, but without any specifics or deadlines. In the following years, the issue was effectively shelved. Only after the start of Russian aggression did the momentum for Ukraine's Euro-Atlantic integration return: in 2019, NATO membership was enshrined in the Ukrainian Constitution, and in September 2022, against the backdrop of Russian attempts to annex Ukrainian territories, our country's leadership submitted a formal application for accelerated accession to the alliance. Ukraine's desire to become a member of NATO currently enjoys unprecedented support among Ukrainian society – about 77% of citizens support joining the alliance. Despite the war, Ukraine has demonstrated its ability and readiness to cooperate closely with NATO. The Armed Forces of Ukraine have effectively transitioned to NATO standards during combat operations and have gained unique combat experience, which they are already sharing with their partners.

At the NATO summit in Vilnius in July 2023, the allies confirmed that Ukraine's future lies in the alliance and waived the requirement to implement the Membership Action Plan on the path to accession, recognising Ukraine's significant progress in reforming its armed forces and achieving interoperability with NATO. The aforementioned Ukraine-NATO Council was established, taking relations to a new level. The Vilnius Communiqué states that NATO 'will be able to send Ukraine an invitation to join when the allies agree and the conditions are met'. In fact, this means that membership will take place as soon as the security situation allows and when all member countries are ready for it. In practice, most NATO allies (especially the countries of Central and Eastern Europe, the Baltic states, and the Scandinavian countries) are in favour of Ukraine's accession as soon as possible, understanding its crucial importance for the long-term stability of the continent. Ukrainian diplomats emphasise that Ukraine, with one of the strongest armies in Europe and vast combat experience, will significantly strengthen NATO and reduce the risk of a repeat of Russian aggression, so there is no point in delaying membership. Experts point out that Europe's security is critically dependent on Ukraine's stability, and that Ukraine's

accession to NATO is the only long-term guarantee of its security [16]. Supporters of accelerated accession also emphasise that Ukraine's prolonged stay outside the alliance only encourages the Kremlin to continue the war, while a clear prospect of membership, on the contrary, will discourage Moscow from further aggression.

At the same time, there are also restraining factors. The main one is the ongoing war in Ukraine. Some Western countries fear that Ukraine's admission to NATO during the active phase of the conflict could drag the alliance into direct war with Russia. Although Kyiv's supporters propose various models such as the 'FRG formula' (when the FRG joined NATO in 1955, but Article 5 was temporarily not applied to the occupied territory of East Germany), some allies still prefer to first achieve at least a stable truce in Ukraine. Another challenge is the position of certain countries (primarily Hungary), which are making political demands – for example, regarding the rights of national minorities – and may slow down the process of reaching a consensus on accession. However, in general, after the Vilnius Summit in 2023, the question of *'whether'* Ukraine will become a member of NATO is no longer relevant; it is only a matter of *'when'*. According to pessimistic estimates, this can only happen after the active phase of the war ends and there is a change of power in Russia; optimists believe that the alliance may take a historic decision as early as the Washington summit in 2025, if by that time the conflict has entered a less intense phase or Ukraine has achieved decisive successes. In any case, Ukraine continues to prepare intensively for accession: it is transitioning to NATO standards, implementing measures for democratic civilian control of the military, and actively involved in joint defence initiatives with NATO.

Politically, Ukraine's accession to NATO is supported by the overwhelming majority of Ukrainian society, and this course has been enshrined in the Ukrainian Constitution since February 2019 as strategic, so there are no internal obstacles in the way – everything depends on the alliance's willingness to accept our country during the ongoing war or immediately after its end.

EU. Unlike NATO, Ukraine's European integration process moved into the practical realm back in 2022, when Ukraine was granted EU candidate status. This decision was momentous both for Ukraine and for the EU itself, which for the first time granted candidate status to a country in a state of major war. Despite some scepticism, Ukraine was able to demonstrate its commitment to reforms even during the hostilities and implemented a

significant part of the European Commission's recommendations necessary to open accession negotiations. In October 2023, the European Commission published a positive report recommending the start of such negotiations. A decision on this is expected from the European Council in late 2023 or early 2024. If negotiations begin, this will open a new phase of legal and economic convergence between Ukraine and the EU, which could last several years.

Full membership of Ukraine in the EU seems entirely realistic in the medium term – this has been openly stated by leaders of key EU member states and institutions. There have been radical changes in the European perception of our country: while there used to be concerns about corruption or the excessive size of the Ukrainian economy, the war has convinced Europe of the strategic necessity of integrating Ukraine. Firstly, the successful expansion of the EU to the East is seen as a tool for strengthening collective security and stabilising Europe's periphery. 'EU enlargement allows the bloc to better strengthen its collective security, stabilise dangerous regions on the periphery and increase resilience to external threats', analysts emphasise [19]. In other words, the accession of Ukraine and other eastern neighbours will make Europe stronger and safer in its confrontation with revanchist Russia. Secondly, Ukraine is already deeply integrated into the EU's economic space thanks to the Association Agreement and the free trade area, as well as the synchronisation of the energy network and the launch of «solidarity routes» for Ukrainian grain exports. This certainly facilitates further integration. Thirdly, Ukraine has great human potential, a resource base and a market, which in the long term is beneficial to the EU itself, especially against the backdrop of Europe's demographic problems. It is no coincidence that even leaders who have traditionally been cautious about enlargement (such as French President Emmanuel Macron) have changed their position after 2022 and openly support Ukraine's future in the EU.

Of course, Ukraine's accession to the EU will not be quick or easy. Our country must fulfil hundreds of conditions and implement a huge body of European law (*acquis communautaire*) in more than 30 thematic clusters of the negotiation dossier. On the agenda are judicial reform, the fight against corruption, the harmonisation of environmental and digital policies, the adaptation of the agricultural sector and other equally important issues. The war complicates these efforts, but does not stop them: the Ukrainian parliament and government continue to pass European integration laws even during shelling. For its part, the EU must prepare for the accession of Ukraine and other new members. This involves internal EU reforms, in particular a

partial abandonment of the principle of unanimity, reforming the common budget and equalisation mechanisms (given the need to finance Ukraine's post-war reconstruction), expanding the composition of governing institutions, etc. For now, there is political will in the EU to move forward: the leadership of the European Commission and the European Council has declared the need for further expansion by 2030, and the countries of the 'old core' (Germany, France, Italy) realise that Europe's security is inextricably linked to Ukraine's membership. Therefore, the main focus is on ensuring that Ukraine continues to successfully implement reforms and demonstrate progress in critical areas (the rule of law, anti-corruption policy, etc.) despite the war. It can be predicted that intensive accession negotiations will continue in the coming years and, in an optimistic scenario, Ukraine will be ready for membership by the end of the decade.

For Ukraine, membership in the EU and NATO is, first and foremost, a guarantee of the irreversibility of its civilisational choice and long-term security. No intermediate formats can replace full membership in these alliances. 'The only real guarantee of security for Ukraine is its full membership in NATO', emphasises the Ukrainian Foreign Ministry, rightly pointing out that, given the bitter experience of Budapest, Kyiv will not agree to 'surrogates' or substitutes for membership [7]. Similarly, EU accession is seen as the only way to rebuild and develop the country's economy in line with European standards. As noted, the vast majority of Ukrainians support Euro-Atlantic integration despite the difficulties and sacrifices involved. Therefore, we can expect that our country will continue to move purposefully towards accession, using its unique status as a 'outpost' of the West to argue for accelerated consideration of its applications by its allies.

28.6. Ukraine's impact on the transformation of the European security order

Ukraine's role in shaping the new European security system is already decisive and will only grow in the future. Thanks to our country's heroic resistance and active stance, fundamental changes have taken place in the priorities and approaches of NATO, the EU and other international institutions. For the first time since the Cold War, European leaders have realised the deadly threat posed by a revanchist Russia and the need to return to a policy of deterrence. NATO has effectively revived its original purpose – to defend the territory of its allies from Russian aggression. The Alliance

has significantly strengthened its eastern flank, increased combat readiness and troop numbers in frontline countries, and developed new long-term defence plans. Influenced by events in Ukraine, European NATO members have finally moved forward on the issue of a ‘European pillar’ of defence: taking into account the prospect of reduced US involvement, EU countries have set a course to strengthen their own defence capabilities within NATO. While only two European NATO countries spent 2% of their GDP on defence in 2022, 22 member states are expected to reach this target by 2024 [1]. This indicates a renewed understanding of the obligation to invest in the continent’s defence.

The EU, in turn, influenced by the war, demonstrated its readiness to take actions that until recently seemed impossible. For the first time in its history, the EU financed the purchase and supply of lethal weapons to a country that was the victim of aggression – which High Representative Josep Borrell called ‘the fall of another taboo’ [20]. This step broke years of restrictions on EU security policy and proved that, for the sake of the principles of freedom and sovereignty, the EU is ready to take ‘joint responsibility’ for the security of its neighbours. The EU also launched new initiatives to strengthen its own defence capabilities: it introduced a joint ammunition procurement programme for Ukraine, allocated funds to expand the production of artillery and air defence systems in Europe, deployed the EUMAM Ukraine military training mission, and actively provides funding for the supply of equipment through the European Peace Fund, etc. Thus, Ukraine’s example has stimulated the development of the EU’s common defence policy, which had been stalled for a long time. In addition, the war in Ukraine has prompted the EU to take radical steps in energy security – abandoning imports of Russian energy resources, searching for alternative suppliers, and accelerating the transition to ‘green’ energy. This deprives the Kremlin of leverage and makes European countries more resistant to blackmail. Moreover, the EU has demonstrated unprecedented unity in its sanctions policy: through its courage and diplomacy, our country has consolidated 27 countries around 16 packages of sanctions against Russia, which was previously difficult to imagine.

In a broader sense, Ukraine has become a kind of ‘litmus test’ for the ability of the Western collective security system to respond to challenges. Despite fears, NATO and the EU have passed this test – largely thanks to the moral example set by Ukrainians. As US Defence Secretary Lloyd Austin emphasised in his speech in Kyiv, the US and its allies have chosen ‘the path

of mutual responsibility and shared security’, sharing with Ukraine the burden of defending freedom [21]. This new principle – the collective responsibility of democratic nations to deter aggression – is becoming decisive for Europe’s renewed security order. In fact, no country can hide behind neutrality when it comes to the fundamental values and stability of the continent. Even traditionally neutral states (Switzerland, Austria) are joining in with sanctions and providing humanitarian aid to Ukraine, understanding that the aggressor threatens everyone.

The Russian-Ukrainian war has caused fundamental shifts in European countries’ approaches to security. Ukraine has found itself at the epicentre of these processes – its struggle not only ensures its own survival, but also determines the future security configuration of the entire continent. As European officials note, the future of the European security order directly depends on Ukraine’s successes or failures on the battlefield [22]. Indeed, if Russia had succeeded in subjugating Ukraine, it would not have stopped there, and the entire system of international law and security in Europe would have suffered a devastating blow. Instead, Ukraine’s heroic resistance not only thwarted the Kremlin’s aggressive plans, but also triggered a chain reaction of change in Europe.

Firstly, NATO has effectively ‘woken up’ after years of relative stagnation. The Alliance has been given a new mission – to defend its eastern borders from a real threat. The accession of Finland (2023) and Sweden (2024) to NATO was an unprecedented step, directly caused by Russia’s aggression against Ukraine. These two countries abandoned their long-standing neutrality, recognising that only collective defence could guarantee their security in the face of the Russian threat. Thus, thanks to Ukraine’s resilience, NATO’s borders have expanded in northern Europe, strengthening the security of the entire Baltic region. Secondly, the EU has demonstrated its capacity for geopolitical mobilisation. Although the EU is not a military alliance, the war has forced Brussels to act as an important security player: new defence initiatives have been launched, including the EU’s first-ever financing of arms supplies (through the EPF fund), coordination of joint replenishment of ammunition stocks for Ukraine, and the creation of a military mission to train Ukrainian troops. As can be seen, the war in Ukraine has forced the EU to radically adapt its common foreign and security policy, revising outdated mechanisms and launching new instruments to strengthen its own defence capabilities. The EU, which at one time hesitated to grant Ukraine candidate status, has now put our country’s accession on the agenda,

recognising that without Ukraine, the project of a united Europe will remain incomplete. Thirdly, Ukraine has significantly influenced the redistribution of roles and priorities within the European community. The countries of Central and Eastern Europe (Poland, the Baltic states, etc.) have gained more weight and influence, as their concerns about the threat from Russia have been fully confirmed. They have become the driving force behind support for Ukraine and 'advocates' for its interests in the EU and NATO, which has shifted the balance of opinion in favour of a more decisive policy of deterrence against Russia. On the other hand, those Western European capitals that had previously relied on 'dialogue' with Moscow are now finally forced to agree on the need for forceful deterrence of the aggressor. The concept of Europe's 'strategic autonomy' has taken on a new dimension: instead of trying to build a security system separate from the US, the EU is focusing on strengthening its own defence capabilities in coordination with NATO in order to have the resources to respond to crises such as the aggression against Ukraine. The war has exposed Europe's critical dependence on external supplies of energy and defence technologies. Accordingly, Ukraine's example has stimulated the EU's accelerated rejection of Russian energy resources and the search for ways to develop its own defence industry.

In addition, Ukraine has transformed from a security consumer country into a security provider country for the region. Today, the Armed Forces of Ukraine are forcibly restraining one of the most powerful armies in the world, thereby indirectly protecting European countries from potential aggression. Representatives of Western countries openly acknowledge that Ukrainians are 'fighting for our freedom'. The Swedish government, in particular, has noted that Ukraine's defeat would be the greatest threat to Europe and to Sweden itself. That is why Europeans continue to increase military aid and sanctions pressure on Russia, understanding that the security of all of Europe depends on Ukraine's victory. In practice, a new security system is already taking shape on the continent, with Ukraine at its centre. As experts rightly point out, the full-scale war against Ukraine has been a critical turning point for European security, after which it will never return to «business as usual» principle. Through its selfless struggle, Ukraine has laid the foundation for a qualitatively new security structure in Europe, based on the strength of democratic alliances rather than shaky agreements with the aggressor.

Ukraine is also setting new standards for resilience and defence that others are using. For example, the Ukrainian model of nationwide defence,

involving civil society, volunteer movements and territorial defence, serves as an example for NATO allies in building their own resilience. Ukraine's experience in countering cyberattacks, disinformation, and energy blackmail by the Russian Federation now forms the basis of EU and NATO strategies to combat hybrid threats. The principle of mutual responsibility is also evident in the fact that NATO countries actively share resources for collective needs, from transferring their own weapons stocks to Ukraine to hosting millions of Ukrainian refugees (more than 8 million Ukrainian citizens have left for the EU since the invasion began). European societies have demonstrated a new level of unity and solidarity, which can also be considered a consequence of Ukraine's influence.

Of course, it is clear that the transformation of the European security order is not yet complete, and Ukraine must make the transition from being a *de facto* «shield» of Europe to a *de jure* full member of Western alliances. This will require further testing of collective security capabilities. Risks remain: if support for Ukraine from its allies weakens or the war drags on without resolution, confidence in collective security could be undermined. However, it is already clear that without Ukraine, a new security order is simply impossible. Ukraine has become a catalyst that has revitalised old institutions (NATO, the EU) and forced them to adapt to new realities. Countries that were hesitant until recently now clearly understand that Europe's security is inextricably linked to Ukraine's security.

Therefore, having considered the transformational processes taking place in the European security system under Ukraine's influence, it seems possible to formulate several strategic conclusions. First, Ukraine has transformed from an object of security policy into an independent force that actively influences the security architecture of Europe. Ukraine's path from partnership to full membership in NATO and the EU has become a catalyst for profound changes in Europe's approaches to its own security and defence. Bilateral security agreements with partners, the acquisition of EU candidate status and the *de facto* rapprochement with NATO all lay the institutional foundations for a new European order in which Ukraine occupies its rightful place as part of the collective West. Secondly, the experience of the Russian-Ukrainian war has convincingly proven the fallacy of old ideas about the possibility of building stable European security without Ukraine or, even more so, against its interests. Despite the terrible price paid daily by the Ukrainian people, it is thanks to Ukraine that it has become possible to «reset» the foundations of European security, in particular the return to the

principles of inviolability of borders and collective defence against aggression. Thirdly, the further evolution of the security system in Europe will directly depend on the outcome of the war and Ukraine's role in the post-war settlement. Ukraine's victory and its integration into NATO and the EU will mark the final collapse of Moscow's imperial ambitions and consolidate a new stable order on the continent. Otherwise, in particular, if the conflict is frozen or Ukraine's sovereignty is not fully restored, the European security order will remain under threat of renewed aggression.

Today, Ukraine is perceived as an integral part of the Euro-Atlantic security space. Our country's contribution to deterring our common adversary, Russia, is already recognised as a key security factor for all allies. It is no coincidence that support for Ukraine has been declared a priority in the foreign and security policies of many European countries. The lessons of war have convincingly demonstrated that without Ukraine, it is impossible to build a strong security system in Europe. Therefore, both NATO and the EU have effectively made a strategic decision to further integrate Ukraine into their ranks – the question is only a matter of terms and conditions. Ukraine, in turn, has proven its readiness to be a reliable ally capable of strengthening collective defence. In view of the above, it can be argued that Ukraine's role in the transformation of the European security order is decisive: our country has moved from the status of a partner to that of a full participant in the new security system, which it helped to win on the battlefield with its own blood. Such a security system, built on the principles of unity, the rule of law and collective resistance to aggression, will be the guarantee of lasting peace and development in Europe for decades to come.

The analysis shows that Russia's war against Ukraine has not only destroyed the old European security system, but has also given impetus to the creation of a new one – one that is more stable, cohesive and responsible. Ukraine has transformed from an object of international politics into a key player that defines the contours of this new system. With their courage and strategic determination, the Ukrainian people have proven their ability to defend their democratic choice, thereby inspiring the entire Western world to consolidate. Thanks to Ukraine, NATO has revived the spirit of collective defence, and the EU has realised the need for geopolitical agency and accelerated expansion. It can be argued that Ukraine has become a catalyst for a paradigm shift: from the concept of «partnership for peace», when the Euro-Atlantic community sought to integrate Russia into the common order,

to a policy of deterrence and mutual support for democracies in the face of an aggressor.

It seems that in the medium term (5-10 years), we should expect the formation of a new security architecture in Europe, with Ukraine playing a central role. Most likely, Ukraine will become a member of NATO as soon as circumstances allow, since Ukraine's military potential and strategic position make it an integral part of collective defence. Our country's membership in the EU seems practically a foregone conclusion and could be realised by the end of the decade, which would strengthen the EU's role as a geopolitical actor. At the same time, Russia, weakened by war and sanctions, will no longer be able to impose its will on Europe if Ukraine is integrated into Western structures. In return, Europe will gain new opportunities, both economic (post-war Ukraine with its large market and resources) and military-strategic (the combat-ready Armed Forces of Ukraine as part of NATO's joint forces).

Thus, Ukraine has gone from being a conditional 'grey zone' to the vanguard of European security. Our country has influenced the revision of key principles of international security, in particular the rejection of appeasement of the aggressor, the return of priority to defence and deterrence, and the affirmation of the principle of the resilience of democratic societies. Ukraine has become the very factor that has united Europe and North America in the face of a common threat, reminding them of the price of freedom and breathing new life into collective security mechanisms. In the new European security system, which is currently being formed in the heat of war, Ukraine is no longer a passive observer, but an equal and influential participant – and a co-creator of the history of the European continent in the 21st century.

References

1. Graham, T. (2024, September). From the Ukraine Conflict to a Secure Europe. *Council on Foreign Relations*. Available at: <https://www.cfr.org/report/ukraine-conflict-secure-europe>
2. Gardner, L. (2025, January 14). European Security: The OSCE at 50. *European Security & Defence*. Available at: <https://euro-sd.com/2025/01/articles/42008/european-security-the-osce-at-50>
3. Factsheet – NATO-Ukraine relations (February 2022). *North Atlantic Treaty Organization*. Available at:

https://www.nato.int/nato_static_fl2014/assets/pdf/2022/2/pdf/220214-factsheet_NATO-Ukraine_Relations_.pdf

4. Партнерство Україна-ЄС у безпековій сфері: сучасний стан і перспективи. К.: Разумков Центр, 2021. 71 с. Available at: <https://razumkov.org.ua/uploads/other/БЕЗПЕКОБЕ%20ПАРТНЕРСТВО%20УКРАЇНА-ЄС.pdf>

5. Helsinki Final Act. August 1, 1975. *Organization for Security and Co-operation in Europe*. Available at: <https://www.osce.org/helsinki-final-act>

6. Charter of Paris for a New Europe. November 21, 1990. *Organization for Security and Co-operation in Europe*. Available at: <https://www.osce.org/mc/39516>

7. Заява МЗС України з нагоди 30-річчя з часу підписання Будапештського меморандуму. *Міністерство закордонних справ України*. Available at: <https://mfa.gov.ua/news/zayava-mzs-ukrayini-z-nagodi-30-richchya-z-chasu-pidpisannya-budapeshtskogo-memorandumu>

8. Balmforth, T. (2022, October 1). Ukraine applies for NATO membership, rules out Putin talks. *Reuters*. Available at: <https://www.reuters.com/world/europe/zelenskiy-says-ukraine-applying-nato-membership-2022-09-30>

9. European Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations. June 23, 2022. *European Council*. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022>

10. Liechtenstein, S. Russia blocks mandate extension of OSCE monitoring mission to Ukraine. *Security and Human Rights Monitor*. Available at: <https://www.shrmonitor.org/russia-blocks-mandate-extension-of-osce-monitoring-mission-to-ukraine>

11. Finnish President of the OSCE's Parliamentary Assembly in trouble after meeting Russian representative. April 12, 2025. *Commonspace.eu*. Available at: <https://www.commonspace.eu/news/finnish-president-osces-parliamentary-assembly-trouble-after-meeting-russian-representative>

12. General Assembly Debates Russian Federation's Security Council Veto of European Amendments Seeking 'Just' Peace in Ukraine. March 06, 2025. No. GA/12677. *United Nations*. Available at: <https://press.un.org/en/2025/ga12677.doc.htm>

13. Gotkowska, J., Nieczytor, K., Graca, J. The West and Ukraine: agreements on security cooperation. *Centre for Eastern Studies (OSW)*. Available at: <https://www.osw.waw.pl/en/publikacje/analyses/2024-01-19/west-and-ukraine-agreements-security-cooperation>

14. Звернення Головнокомандувача Збройних Сил України генерал-полковника Руслана Хомчака з нагоди Дня створення Організації Північноатлантичного договору. 04 квітня 2021 р. *Генеральний штаб ЗСУ: офіційна сторінка у Facebook*. Available at: <https://www.facebook.com/GeneralStaff.ua/posts/1888974117938503>

15. Watson, E., Martin, D. (2022, May 6). Intelligence provided by the U.S. helped Ukrainians sink Russian ship Moskva. *CBS News*. Available at: <https://www.cbsnews.com/news/moskva-ship-sink-russia-ukraine-us-intelligence>

16. Спільна декларація про підтримку України. 12 липня 2023 р. *Офіційне інтернет-представництво Президента України*. Available at: <https://www.president.gov.ua/news/spilna-deklaraciya-pro-pidtrimku-ukrayini-84277>

17. Угода про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії. 12 січня 2024 р. *Офіційне інтернет-представництво Президента України*. Available at: <https://www.president.gov.ua/news/ugoda-pro-spivrobotnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-88277>

18. Podvorna, O. (2024, October 17). Sweden's Accession to NATO: What Is behind the Decision? *PRIF blog*. Available at: <https://blog.prif.org/2024/10/17/swedens-accession-to-nato-what-is-behind-the-decision>

19. Morina, E. (2025, April 14). Stumbling blocs: Why the EU's future security depends on successful enlargement. *European Council on Foreign Relations*. Available at: <https://ecfr.eu/article/stumbling-blocs-why-the-eus-future-security-depends-on-successful-enlargement>

20. Bartoloni, M. E. (2022). First-Ever EU Funding of Lethal Weapons: "Another Taboo Has (Lawfully) Fallen". *European Papers*. 7(1), 379–383. Available at: <https://www.europeanpapers.eu/europeanforum/first-eu-funding-of-lethal-weapons-another-taboo-has-lawfully-fallen>

21. Remarks in Kyiv by Secretary of Defense Lloyd J. Austin III on Ukraine's Fight for Freedom. October 21, 2024. U.S. Embassy in Ukraine. Available at: <https://ua.usembassy.gov/remarks-in-kyiv-by-secretary-of-defense-lloyd-j-austin-iii-on-ukraines-fight-for-freedom>

22. Genini, D. (2025). How the war in Ukraine has transformed the EU's Common Foreign and Security Policy. *Yearbook of European Law*. 1–43. Available at: <https://academic.oup.com/yel/advance-article/doi/10.1093/yel/yeaf003/8112000>

Chapter 29

Transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU (I. Zablodska, Y. Dyakon, P. Lyashenko)

The transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU provides for the modernization of the economic space in the de-occupied territories, which is aimed at integrating these regions and territorial communities into the national and European economic system, using the principles, standards and financial instruments of the European Union.

The problems of transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU are actively studied by domestic scientists and experts, among whom scientists from the State Institution 'V.K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine' and Volodymyr Dahl East Ukrainian National University [1–5] should be singled out.

The study of these issues is the purpose of this chapter.

29.1. Restoration and reconstruction of infrastructure

The process of restoration and reconstruction of infrastructure in the de-occupied territories in the context of Ukraine's integration into the EU includes a whole range of targeted organizational, engineering, technical, financial, economic and social measures aimed at recreating and modernizing transport, energy, municipal, social and digital infrastructure facilities that were damaged or destroyed as a result of hostilities and occupation. In Table.

29.1 Conceptual triggers for the process of restoration and reconstruction of infrastructure in the de-occupied territories are presented.

Table 29.1

Conceptual triggers for the process of restoration and reconstruction of infrastructure in the de-occupied territories*

Triggers	Meaningful content
Restitution of basic life support functions	restoration of electricity, water and heat supply, communications, transport corridors, etc.
Innovation and technological modernization	implementation of modern, energy-efficient, digital and environmentally sustainable solutions, etc.
Institutional and legal support	creation of reconstruction management mechanisms, transparent financing procedures, public-private partnership, etc.
Social and humanitarian aspect	ensuring the return of the population, the restoration of social infrastructure, and improving the quality of life.

**Source: compiled by the authors based on [1-5]*

Restoration and reconstruction of infrastructure is a basic prerequisite for sustainable economic growth, national security and successful post-war integration of the de-occupied territories into the national and international economic space. However, the primary task of transforming the economic space in the de-occupied territories is the reconstruction of critical infrastructure destroyed as a result of hostilities: the restoration of the transport network involves the restoration of roads, bridges, railways and logistics hubs to ensure the free movement of goods and services; restoration of energy infrastructure is the repair and modernization of power grids, substations, gas and water supply; The restoration of social infrastructure is the reconstruction of hospitals, schools, kindergartens, residential buildings and administrative buildings.

The restoration and reconstruction of critical infrastructure will affect local economic development through improved transport accessibility, which will reduce logistics costs for businesses, increase the speed and reliability of turnover, and contribute to the expansion of sales markets. Increasing the infrastructural attractiveness of the region and territorial communities will help reduce risks and improve the conditions for doing business, which will improve the quality of life of the population, including through the restoration of social, communal and energy infrastructure, which, in turn, will stimulate the return of people to the de-occupied territories.

29.2. Economic recovery and development

Economic recovery of the de-occupied territories includes stimulating the economic activity of business entities: supporting business through the provision of soft loans, grants and tax incentives for small and medium-sized businesses that resume their activities or start a new one; attracting investment and creating a favorable investment climate, including the protection of property rights, security guarantees and clear regulatory rules harmonized with European legislation; the return of enterprises to the de-occupied territories or the creation of conditions for the restoration of businesses that were forced to stop work, and its further integration into the local economy of the region or territorial community, etc.

The economic recovery and development of the de-occupied territories also depend on the activity of humanitarian demining of the territories of these regions or territorial communities.

Humanitarian demining is a set of measures aimed at detecting, identifying, neutralizing and removing explosive ordnance from the de-occupied territories in order to ensure the safety of the population, restore socio-economic activity and protect the environment. Unlike military demining, which has a tactical or operational goal (creating safe passages for troops), humanitarian demining is focused on the civilian environment and includes not only technical works, but also educational-preventive and socio-economic components.

A fragment of the system of predictors of humanitarian demining in the context of the transformation of the economic space in the de-occupied territories is shown in Fig. 29.1.

The system of predictors of humanitarian demining includes indicators, factors and variables that make it possible to predict the volume, pace, priority and socio-economic consequences of demining, as well as integrate them into the strategies for the reconstruction and development of regions after de-occupation. In such a system, predictors play the role of 'signal variables' that allow: to assess the degree of danger of the territory (density and types of explosive objects, the level of soil contamination); to predict the economic effect of land clearance (return of agricultural land, launch of production facilities, restoration of transport routes); prioritize demining to ensure the rapid restoration of critical infrastructure; assess the social impact (level of security for the population, the possibility of returning IDPs, restoring access to services); take into account institutional and financial

conditions (availability of international support, legal mechanisms, personnel and technical support).

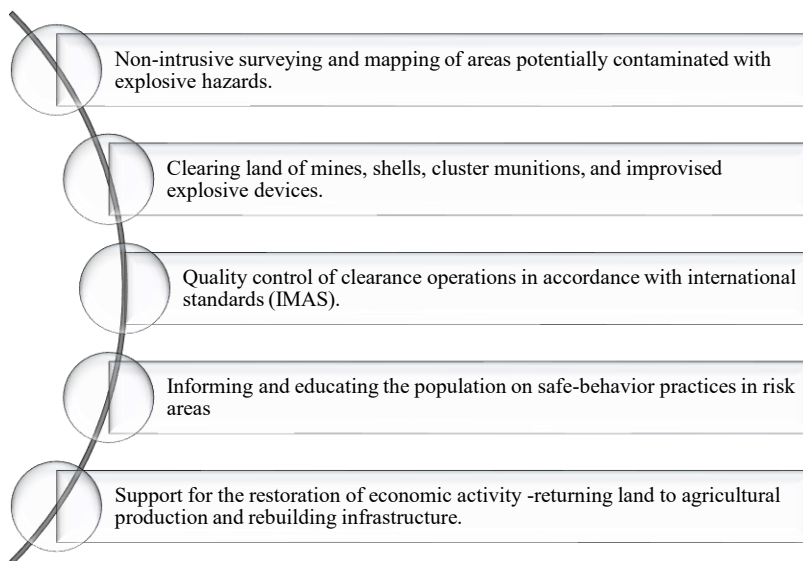


Fig. 29.1. Fragment of the system of predictors of humanitarian demining in the context of transformation of the economic space in the de-occupied territories

Source: compiled by the authors based on [1-5]

In the context of the transformation of the economic space in the de-occupied territories, the system of predictors of humanitarian demining becomes a tool for strategic planning, as it makes it possible to combine the technical logic of humanitarian demining with economic priorities: to intensify the economic activity of the agricultural sector, restore logistics corridors, encourage investment activity and integrate regions into the national and European economic space.

Therefore, the restoration of the territories of Ukraine affected by Russian aggression is unrealistic without large-scale and effective demining. This process is not only a humanitarian task, but also a critical economic and security challenge. In order to improve economic approaches to demining in the face of current challenges and threats to the national security of Ukraine, researchers have developed a number of proposals.

1. *Introduction of a three-tier system of demining prioritization.* Due to the lack of resources, demining of all contaminated territories at the same time is impossible. An effective economic approach requires a clear prioritization of the territories to be demined. The demining prioritization system contains three levels and is based on an assessment of the potential of land use, Fig.29.2. This approach will allow directing limited financial and human resources to the most strategically important plots of mined areas, maximizing the economic effect of each hryvnia spent.

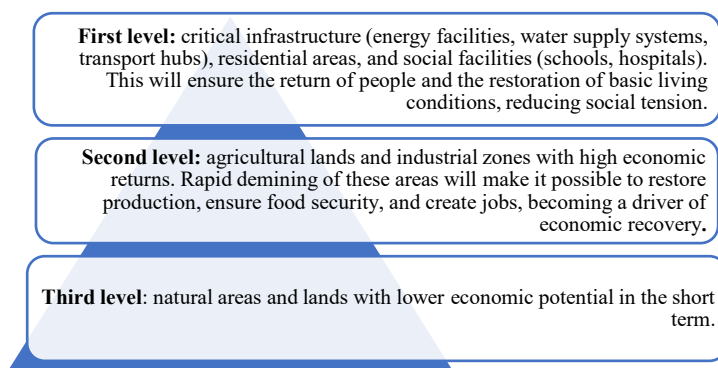


Fig. 29.2. Levels of demining prioritization

Source: compiled by the authors based on [1-6]

2. *Creation of the Public-Private Fund for Demining and Reconstruction.* Financing of demining requires significant funds that go beyond the capabilities of the state budget, especially in wartime. interested in the further use of demined areas. For example, large agricultural holdings can finance the demining of their lands in exchange for tax benefits), donor contributions (attracting charitable foundations and private donors). Such a State Pension Fund will ensure transparency in the distribution of funds and allow diversification of risks, reducing dependence on a single source of funding.

In Ukraine, amendments have already been made to some legislative acts of Ukraine to improve the mechanism for attracting private investment using the mechanism of public-private partnership to accelerate the restoration of objects destroyed by the war and the construction of new objects related to the post-war restructuring of the economy of Ukraine [6]

3. Introduction of tax and regulatory incentives for private operators.

The involvement of the private sector will significantly speed up the demining process. Now it is carried out mainly by state and international organizations, but it is necessary to improve the business environment for private firms by providing: tax holidays, i.e. exemption from income tax for companies engaged in demining for the first 5-10 years; preferential lending, i.e. providing access to cheap loans for the purchase of equipment; government orders through the conclusion of long-term contracts with clear tariffs and guarantees; simplified licensing procedure and maximum simplification of bureaucratic procedures for obtaining work permits, etc.

4. Development of domestic production of demining equipment.

Dependence on the import of specialized equipment (demining robots, drones with sensors, protective equipment) is expensive and vulnerable. Setting up own production is of strategic importance, since there is an economic benefit, i.e. a reduction in the cost of equipment, a reduction in delivery and service times, which will also stimulate the development of the domestic military-industrial complex and engineering, accessible regardless of geopolitical circumstances. It is important to diffuse innovations through research centers that will develop new, more effective demining technologies, taking into account the specifics of Ukrainian territories.

5. Intensification of the work of the unified information register. The lack of centralized data or their absence creates chaos and reduces the effectiveness of demining measures. The Center for Humanitarian Demining contributes to the restoration of a safe environment, which is a key factor for economic reconstruction and community development [7].

6. Improvement of mechanisms for insuring war risks and investments in demined areas. Potential investors and farmers will not dare to invest in demined areas if there is a risk of their re-contamination or damage from incomplete demining. Therefore, the state insurance program should guarantee compensation for losses in case of detection of explosive ordnance after official demining. Partnership with international insurance companies should involve international insurance giants for reinsurance, which will increase investor confidence. business, which is a key factor in attracting long-term investments.

7. Integration of demining into regional and municipal recovery strategies. Demining cannot be a separate process that is of interest only to the state. It should be part of the state recovery strategy, as well as the strategies of regions and territorial communities, which are developed at the

local level. Local authorities should integrate demining plans into community development master plans, taking into account the needs of businesses and residents. Coordinate efforts between different stakeholders – military, humanitarian organizations, private companies and communities. demining of land, territories will immediately be ready for use for development, agricultural production or industrial parks, which will reduce the ‘downtime’ of assets.

8. Development of the system of training and retraining of demining specialists. The acute shortage of qualified sappers is one of the biggest deterrents. The creation of new training centers will expand the network of training centers that meet international standards. And funding of training at the expense of the state, followed by mandatory training, will provide high salaries, social protection and benefits for specialists working in this dangerous field, which will strengthen high-quality human capital as the basis for fast and safe implementation works.

9. Creation of special economic zones ‘mine-free’. To accelerate economic growth in the de-occupied territories, it is necessary to create ‘islands of stability’. These are local territories exempt from tax or customs benefits, providing businesses located on these ‘islands’ with special economic conditions state. This approach will allow you to quickly attract investments, create jobs and strengthen the economic potential of the regions.

10. Involvement of remote demining technologies and artificial intelligence. Manual demining is a slow and dangerous type of demining. The use of modern technologies will significantly increase the efficiency of demining. Modern remote demining technologies include: robotic systems (the use of robotic machines, demining drones and other technologies will allow processing large areas faster and with less risk to the lives of sappers); artificial intelligence (AI) (the use of AI to analyze data received from drones and satellites, will allow you to create accurate maps of minefields and predict hazardous areas). The development of remote demining technologies requires large investments that will allow Ukraine to become a world leader in the field of demining, exporting its knowledge and technologies to other countries that have faced and will face similar challenges.

The proposals for improving economic approaches to demining in the face of current challenges and threats to Ukraine's national security are complementary to other measures aimed at transforming the demining process from a humanitarian burden into a catalyst for the transformation of

the economic space in the de-occupied territories in the context of Ukraine's integration into the EU.

29.3. Harmonization of legislation and standards with the EU

The harmonization of legislation and standards of Ukraine with the EU is carried out through the implementation of European law into national legislation, which is a decisive stage on the way to full membership in the European Union. This process covers various areas and is carried out through several main mechanisms:

the adaptation process involves amendments to the current Ukrainian legislation, as well as the adoption of new laws that comply with European standards, this applies to both legislative acts (laws, resolutions, decrees) and by-laws (regulatory) documents;

Ukraine is gradually abandoning outdated post-Soviet standards (GOST, DSTU) in favor of European (EN). This synchronization is critical for: increasing competitiveness (Ukrainian goods and services become more competitive in the European market, as they meet generally recognized requirements) and export facilitation (technical barriers to trade are eliminated, which allows Ukrainian manufacturers to export their products to EU countries more easily);

For the effective implementation of European legislation, reforms of state institutions are needed, which should ensure proper implementation and control over compliance with the new rules. Which includes: judicial reform (ensuring the independence of the judiciary, which is a guarantee of the protection of property rights and investments) and public administration reform (creation of effective, transparent and accountable bodies that meet European governance standards);

Various instruments and mechanisms are used to support the harmonization process, in particular: the Association Agreement between Ukraine and the EU (is the main document that defines the roadmap for reforms and contains a list of legislative acts that Ukraine has undertaken to implement); financial assistance (the European Union provides Ukraine with financial and technical assistance for the implementation of harmonization reforms); Programs and projects (participation in joint programs (e.g. Horizon Europe, Erasmus+) contributes to the exchange of experience and integration into the European scientific, educational and economic space).

That is, harmonization is a complex process that includes legislative, institutional and economic transformations aimed at the full integration of Ukraine and its de-occupied territories into the EU single market in order to achieve compliance with all membership criteria.

In the de-occupied territories, this process is taking place in unison with the whole state, but with an emphasis on the following areas: the introduction of European standards, i.e. product quality standards, environmental, technical and sanitary standards, which will facilitate exports to the EU countries and promote integration into the European single market; anti-corruption measures, strengthening the fight against corruption, transparency in the distribution of financial resources for reconstruction and development; implementation of reforms in the areas of public administration, justice and the financial sector, which are key to EU membership.

29.4. Human Capital Development and Social Inclusion

Successful transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU is impossible without the restoration of human potential. The development of human capital and social integration in the de-occupied territories in the context of Ukraine's integration into the EU are carried out through the implementation of comprehensive programs aimed at restoring and strengthening the social sphere, education, health care and the labor market. This is a critical aspect of recovery, as sustainable economic growth is impossible without human potential. In Table. 29.2 presents the triad (its components and description) of the development of human capital and social integration in the de-occupied territories of Ukraine.

Thus, the transformation of the economic space in the de-occupied territories is a strategic direction of Ukraine's recovery, which should be carried out taking into account European values, norms and principles to ensure its successful integration into the European Union. In fact, such a transformation is not only a process of restoring destroyed economic structures, but also a transition to a qualitatively new level of development, in which the de-occupied territories become an integrated part of the single European economic space.

Table 29.2

The Triad of Human Capital Development and Social Integration in the De-Occupied Territories*

Triad	Ingredients	Description
Education and vocational training	Restoration and modernization of educational institutions	reconstruction of schools, kindergartens, colleges and universities that were destroyed or damaged. Equipping them with modern equipment
	Retraining programs	launching short-term training courses (retraining programs) for people who have lost their jobs or whose skills have become irrelevant. These programs are focused on meeting the needs of the new, renewed labor market, in particular in the fields of construction, IT, services and the agricultural sector.
	Scholarships and grants	providing financial support to students and apprentices to encourage them to study and acquire new professions.
Health and psychological support	Restoration of medical infrastructure	repair and construction of hospitals, clinics and paramedic and obstetric centers. Providing them with the necessary medical equipment and medicines.
	Psychological assistance	provision of free psychological and rehabilitation services for the population, especially for veterans, their families and survivors of the occupation.
Social integration and support of the population	Support for internally displaced persons	creating conditions for the return and reintegration of IDPs, including housing, job search assistance, and access to social services.
	Programs for veterans	development of special programs of social adaptation, training and employment for veterans returning to civilian life
	Providing access to services	resumption of the work of administrative service centers, bank branches, post offices and other vital services.
	Community Development	involvement of the local population in decision-making processes for the reconstruction and development of their communities. What contributes to increasing social cohesion and responsibility

**Source: compiled by the authors based on [1-5]*

29.5. Reconfiguration of the administrative-territorial structure in the de-occupied and affected territories

An important aspect of restoring the economic space of Ukraine in the post-war period and ensuring Ukraine's integration into the EU is the creation of preconditions and solving practical problems for the effective and effective functioning of local self-government bodies in the de-occupied and affected territories. The management system of local self-government bodies must be able to respond mobily and effectively to changes taking place in territorial communities and the state, i.e. to function effectively and effectively. This is

especially true for communities in the de-occupied territories, as well as territories where active hostilities are taking place [8, p. 61].

The reconfiguration of the administrative-territorial structure (ATU) in the de-occupied and affected territories of Ukraine involves taking into account the arguments presented in Fig. 29.3.

Therefore, the restoration or change of the boundaries of communities and districts should take into account demographic changes, the volume of destruction of infrastructure and logistics corridors, the destruction of settlements, etc.

The adaptation of the management system should be aimed at new security and economic realities, including the creation of special management regimes (for example, transitional administrations or military-civilian administrations).

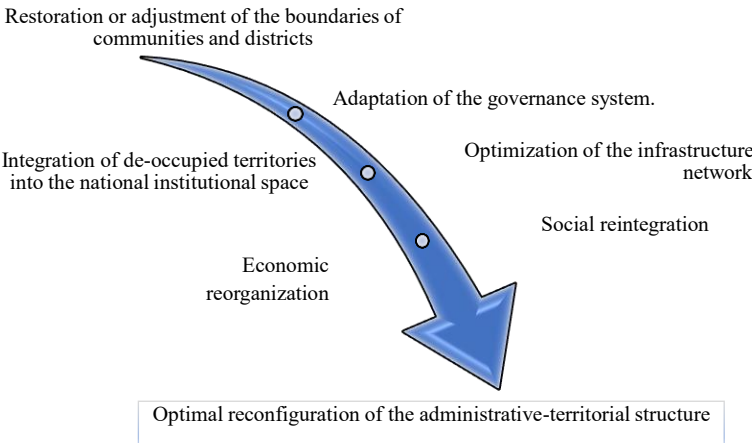


Fig. 29.3. Arguments in favor of the reconfiguration of ATS in the de-occupied and affected territories of Ukraine

Source: compiled by the authors

The integration of the de-occupied territories into the national institutional space will take place through the resumption of the work of authorities, law enforcement agencies and the judicial system.

Optimization of the infrastructure network to ensure the population's access to basic services covers healthcare, education, utilities, and transport links.

Economic reorganization involves the restoration of the tax base, the formation of local budgets, the launch of economic activity, adaptation to reconstruction and investment support programs.

Social reintegration is aimed at creating conditions for the return of internally displaced persons and the restoration of social infrastructure.

Thus, the reconfiguration of ATU in these territories is not only a territorial and legal issue, but also a tool for comprehensive restoration and safe integration of regions into the political, economic and social space of Ukraine and the EU.

Researchers of the Luhansk branch of the State Institution ‘V.K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine’ and Volodymyr Dahl East Ukrainian National University in 2023–2024 assessed the capacity of communities of Donetsk and Luhansk regions in the transition period after de-occupation using the proposed indicators: the number of people permanently residing in the territory of a capable territorial community, the number of students receiving education in general secondary education institutions located in the community, and the share of the able-bodied population permanently residing in the territory of a capable territorial community. Scientists have identified an optimistic, real and pessimistic scenario of reconfiguration of the administrative-territorial structure of Donetsk and Luhansk regions at the level of communities and districts after de-occupation [8, p. 60–68.].

The following studies on the reconfiguration of ATU in Kharkiv, Zaporizhzhia, and Kherson regions in 2025 were carried out within the framework of the project ‘Formation of Conceptual Legal Foundations for the Institutional Restoration of Donbas’, based on the results of cooperation between the NGO ‘Association for the Promotion of Self-Organization of the Population’, the NGO ‘Center for Political and Legal Reforms’, the NGO ‘Public Initiative of Luhansk Region’ and the NGO ‘Association ‘Renaissance and Development’ and with the support of the International Renaissance Foundation [9].

The analytical studies carried out and recommendations for the reconfiguration of territorial communities and districts under two scenarios are the basis for the reconfiguration of ATU in Zaporizhzhia, Kharkiv and Kherson regions and can be used to transform the economic space in the de-occupied territories in the context of Ukraine’s integration into the EU.

29.6. Legislative initiatives aimed at the restoration and development of territories

Economic recovery.

Scientists of the Luhansk branch of the State Institution ‘V. K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine’ actively participated in the development of a regulatory framework for the restoration and development of the affected territories. Because the problems of introducing incentives for economic activity for the restoration of the de-occupied territories, territories adjacent to the line of hostilities have been repeatedly resolved in various draft laws of Ukraine. However, if before At the beginning of the full-scale invasion, such draft laws provided for the creation of special regimes of economic activity in the territory of Donetsk and Luhansk regions, therefore, due to the expansion of hostilities and shelling of infrastructure throughout Ukraine, the temporary occupation of the territories of other regions, legislative initiatives on economic development with reference to the administrative boundaries of territorial units are not initiated today.

Among the draft laws submitted before February 24, 2024, the most comprehensive and successful was the legislative initiative developed based on the results of comprehensive consultations between the People’s Deputies of Ukraine – members of various Committees of the Verkhovna Rada of Ukraine, representatives of the Government and the expert community. We are talking about the draft Law of Ukraine Register No. 6403 of 07.12.2021 ‘On the introduction of a special regime of economic activity in the territory of priority development in Donetsk and Luhansk regions’ [10]. The draft law not only proposed to regulate the basic principles of the creation and operation of a special regime of economic activity in the territory of priority development in Donetsk and Luhansk regions (hereinafter referred to as TPR), requirements for residents, control and monitoring of compliance with the current legislation, it introduced three-level state support with separate features for different territories: 1) the entire territory of Donetsk and Luhansk regions, with the exception of temporarily occupied territories (regional level); 2) territories of territorial communities adjacent to temporarily occupied territories (level of territorial communities adjacent to temporarily occupied territories); 3) territories of industrial parks (level of industrial parks). This draft Law provided for the creation of an international Consortium Financing Fund in order to raise funds for the purpose of

infrastructure restoration and/or financing other measures to stimulate economic activity in the TPR, the introduction of an insurance system against military-political risks, as well as the possibility of referring disputes involving a foreign investor or non-resident to international commercial arbitration. Due to the full-scale invasion, these draft laws were not considered, since the problems that were once relevant for the territory of the two regions have become problems for many regions.

At the same time, the ideas and developments laid down by these draft laws are reflected in the draft laws of Ukraine, which are currently under consideration by the Verkhovna Rada of Ukraine and the expediency of considering which are supported by the Government. Among them:

- draft Law of Ukraine register. No. 12372 of 20.12.2024 ‘On the War Risk Insurance System’ [11], which proposes the creation of a war risk insurance system and the regulation of the activities of the subjects of such an insurance system;

- draft Law of Ukraine register. No. 13414 of 26.06.2025 ‘On Amendments to Paragraph 4 of Section XXI ‘Final and Transitional Provisions’ of the Customs Code of Ukraine on Compensation of Investments through Taxes’ [12] and the register. No. 13415 of 26.06.2025 ‘On Amendments to Section XX ‘Transitional Provisions’ of the Tax Code of Ukraine on Compensation of Investments through Taxes’ [13], which contain provisions on exemption from corporate income tax, VAT and duties on the import of equipment, as well as exemption from land tax and land rent.

The adoption of legislative acts that will be harmonized with the legislation and will meet EU standards and which will be aimed at creating measures to support the development of economic potential, restore damaged or destroyed production facilities, rebuild and develop regions where hostilities were conducted and/or were temporarily occupied, is an important direction of state policy and requires concerted actions on the part of the legislative and executive branches of government. At the same time, Ukraine, when developing approaches to stimulating economic recovery and the development of regions and individual industries, in particular, should take into account the consequences of armed aggression and apply various types of incentives: both the introduction of tax and other incentives for certain industries, and the introduction of features to support economic activity in certain territories.

Social and humanitarian aspect

The restoration and reconstruction of infrastructure and production facilities in the de-occupied territories is not possible without the availability of labor resources in such regions. And along with tax and other incentives for sectors of the economy and industries, the state must ensure the return of the population, restore social infrastructure, and provide the population with housing.

Given that more than 11 million people have been displaced in Ukraine, of which about 5 million are internally displaced persons and more than 6 million are persons who have left Ukraine, special attention should be paid to their return to their abandoned place of residence.

The current legislation, including the Law of Ukraine No. 1706-VII of 20.10.2014 ‘On Ensuring the Rights and Freedoms of Internally Displaced Persons’, does not provide for the implementation of measures for the reintegration of the population after returning to the abandoned place of residence. Law No. 1706 provides only for the assistance of return, such as the possibility of free travel to the abandoned place of residence and assistance from local authorities in the transportation of movable property. Due to the outdated provisions of Law No. 1706, which do not correspond to the situation that developed after the full-scale invasion, work began on its new version in July 2023.

Currently, the draft Law of Ukraine Register has been registered and adopted in the first reading. No. 12301 of 11.1.2024 ‘On Amendments to the Law of Ukraine ‘On Ensuring the Rights and Freedoms of Internally Displaced Persons’ and Other Laws of Ukraine’ [14], which sets out the Law No. 1706 in a new edition, introduces at the level of the law such concepts as integration and reintegration, determines that the state provides assessment of the needs of internally displaced persons and monitoring the satisfaction of such needs, and provides support at all stages of internal displacement, including when returning to an abandoned place of residence and further reintegration.

Article 27 of this draft law defines the main areas of state support during reintegration, in particular, the restoration of individual rights, the provision of housing, the promotion of employment and the requalification of ensuring the provision of social and other services, etc.

Thus, the adoption of this Law and ensuring the adoption by the Government of the relevant regulations for its implementation will create the necessary grounds for the implementation of all components of the triad of

human capital development and social integration in the de-occupied territories, given in Table. 29.2.

At the same time, the restoration of power and the reconstruction of institutions in the de-occupied territories should be carried out. At one time, the Government submitted to the Verkhovna Rada of Ukraine the draft Law of Ukraine Reg. No. 5844 of 09.08.2021 'On the Principles of State Policy of the Transition Period' [15], which, as stated in the explanatory note, was supposed to 'determine a certain algorithm of actions of the state during the reintegration of the temporarily occupied (de-occupied) territories and their residents, the de-occupation of the temporarily occupied territories, including the issues of demilitarization and disarmament, solving humanitarian problems, restoring justice, etc.'

However, this draft law was withdrawn on January 25, 2025 and today there is a need for the Government to submit relevant legislative initiatives of state policy regarding the temporarily occupied territories, the process of de-occupation, restoration of power and support for citizens living in and returning to such territories.

One of the main problems of returning to the de-occupied territories and attracting additional labor resources through the migration of the population from other regions, along with security, employment and decent wages, is the problem of housing availability. In this direction, legislative initiatives aimed at providing citizens with compensation for property destroyed or damaged since February 19, 2014, the introduction of remote inspection of damaged and destroyed property in the territory of hostilities and temporarily occupied territories, and the comprehensive restoration of apartment buildings can contribute to solving the issue of ensuring housing rights. Such norms, among others, are contained in the draft law register No. 13136 of 26.03.2025 'On Amendments to of the Law of Ukraine 'On Compensation for Damage and Destruction of Certain Categories of Real Estate Objects as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine, and the State Register of Property Damaged and Destroyed as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine' and some other laws of Ukraine on improving the mechanism for providing compensation and accounting for real estate property' [16].

It is also important to resolve the issues of providing compensation in the case when settlements are destroyed (the infrastructure of which is destroyed and damaged to such a state that such settlements are

uninhabitable), which, among other things, is proposed by the draft law register. No. 11444 of 26.07.2024 ‘On Amendments to Certain Laws of Ukraine on Improving the Legal Regulation of Issues Related to Compensation for Damage and Destruction of Certain Categories of Real Estate as a result of the armed aggression of the Russian Federation against Ukraine and the maintenance of the State Register of Property Damaged and Destroyed as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine’ [17].

Having decided on the policy of the state regarding the provision of compensation for objects that were destroyed or damaged as a result of armed aggression in the period up to February 22, 2024, regarding the identification of destroyed (uninhabitable) settlements, regarding the provision of compensation not only in the form of money, but also through the comprehensive restoration (reconstruction) of apartment buildings, and having data on destroyed property in the temporarily occupied territories based on the results of remote inspection, when preparing strategies and plans for the restoration of the de-occupied territories, the Government will have the necessary data on the needs for reconstruction, the feasibility of restoring individual settlements or parts of them, methods and the approximate need for financial resources for the reconstruction of housing and infrastructure.

Based on this, and taking into account the availability of natural resources, surviving production capacities, social infrastructure and logistics routes, even before, or in a short time after, de-occupation and before the start of the restoration of the region, it is possible to determine the formation (liquidation) of settlements, the establishment (change) of their boundaries, the assignment of settlements to another category in accordance with the Law of Ukraine No. 3285-IX of 28.07.2023 ‘On the procedure for resolving certain issues administrative-territorial structure of Ukraine’ and, accordingly, adjust and optimize plans for the restoration and development of the de-occupied territories.

At the same time, it is important to ensure that records are kept of all losses caused as a result of armed aggression against Ukraine, and not only damaged or destroyed housing. Therefore, it is important to fill the Register of Property Damaged and Destroyed as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine (hereinafter referred to as the RPZM) with information on all real estate and movable property, as provided for in the current legislation, taking

into account the clarifications proposed by the draft Register. No. 13136 of 26.03.2025, which clarifies these norms and strengthens the obligation to comply with them.

Also, an important component for understanding the damages caused, in the context of regions, industries, residential, social, transport and other infrastructure, should be the reflection in the RPMP of information on material damage (including damages) caused not only to property owners, but also to managers of residential buildings, providers and performers of communal services, state authorities, local self-government and legal entities (tenants, users, service providers organizations, etc.) as a result of damage and/or destruction of property (primarily apartment buildings). This is the register provided for by the draft law. No. 13155 dated 13.05.2025 ‘On Amendments to Certain Laws of Ukraine Regarding the Accrual of Payment for Housing and Communal Services and Accounting for Losses in Connection with Damage or Destruction of Real Estate’ [18].

This draft law was developed to settle possible disputes between property owners and management companies or utility providers in the event of destruction or damage to an apartment building. When preparing the draft law for the second reading, proposals were received from people's deputies of Ukraine to take into account in this draft also existing problems regarding the provision of housing and communal services, gas, water and heat supply and the settlement of disputes regarding the occurrence and settlement of debts on facilities located in the territories where hostilities are taking place or which were temporarily occupied.

Such initiatives are important for making appropriate decisions on the restoration of infrastructure and housing and communal services in the de-occupied territories. Even if they are not supported in the draft law, the register. No. 13155 of 13.05.2025, then we should expect relevant legislative initiatives from the Government.

Given that not all damaged and destroyed facilities will be restored, as well as taking into account the fact that in the event of migration of labor resources to the de-occupied regions, there will be a need for additional housing, changes in state housing policy are urgent. As a result of the provisions of the outdated Housing Code, which expanded the possibilities of privatization of service and social housing, today there are no housing funds in territorial communities that can be used for the purpose of temporary residence, or as social or service housing.

Draft Law of Ukraine Register. No. 12377 of 06.01.2025 'On the Basic Principles of Housing Policy' [19] changes the existing approaches and introduces the basic principles of the formation of service and social housing funds using public-private partnership mechanisms. Its adoption will make it possible to submit the draft Law of Ukraine 'On Social Housing Fund' as soon as possible and lay the foundations for the development of the social (affordable) rental market.

Given the significant damage to the housing stock, these mechanisms for providing temporary, social and service housing will become the main way to quickly solve the housing issue in the de-occupied territories and will make it possible to attract additional labor resources to these regions.

Thus, the transformation of the economic space in the de-occupied territories in the context of Ukraine's integration into the EU is a strategic task of the state recovery policy. Its implementation involves a set of measures: reconstruction of critical infrastructure, stimulation of economic activity, humanitarian demining, harmonization of legislation with EU standards, development of human capital and social integration, etc. An important element is the reconfiguration of the administrative-territorial structure, which will allow adapting the management system to new demographic and security conditions. Legislative initiatives aimed at supporting business, restoring housing and ensuring the social rights of citizens create institutional foundations for the sustainable development of regions. Thus, the transformation of the de-occupied territories is not only restorative, but also integrative, as it is aimed at including these regions in the common European economic and legal space, which forms the prerequisites for long-term stability and prosperity of Ukraine.

References

1. Zablodska, I. V., Grechana, S. I., Kovalchuk, E. O. (2024). Coherence of Sustainable Construction and Local Economic Development in the De-Occupied and Affected Territories. *Regional Economy*. No4 (114). Pp. 39–51. <https://doi.org/10.36818/1562-0905-2024-4-5>
2. Pletnev, M. V. (2022). Transformation of the Economic Space of Ukraine through the War. *Journal of Economic Reforms*. № 2 (46). Pp. 25–30. <https://doi.org/10.32620/cher.2022.2.04>
3. Sieriebriak, K., Zablodska, I., Bielousov, Y. (2025). Theoretical and methodological foundations spatial development // *Modernisation of the*

Economy and Financial System: Problems, Opportunities, Prospects: Collective monograph. Part 2. Riga, Latvia: Baltija Publishing, 2025. P.172–223. <https://doi.org/10.30525/978-9934-26-540-2-28>

4. Preservation and development of Ukraine in the conditions of war and peace: national report / ed. coll. S. I. Pyrozhkov, N. V. Khamitov, E. I. Holovakha, S. S. Dembitsky, E. M. Libanova, O. V. Skrypniuk, S. V. Stoyetsky, I. V. Zablodska. Institute of State and Law. V. M. Koretsky of the National Academy of Sciences of Ukraine. Kyiv, 2024. 220 p. Available at: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/65375/1/240.pdf>

5. Buzko, I., Zablodska, I., Bielousov, Y. (2025). Theoretical foundations of regional development in the context of spatial transformations // Modernisation of the Economy and Financial System: Problems, Opportunities, Prospects: Collective monograph. Part 2. Riga, Latvia: Baltija Publishing, P.120–171. <https://doi.org/10.30525/978-9934-26-540-2-27>

6. On the adoption as a basis of the draft Law on the State Budget of Ukraine for 2023: Resolution of the Verkhovna Rada of Ukraine dated 06.10.2022 No. 2648-IX. Verkhovna Rada of Ukraine. Available at: <https://zakon.rada.gov.ua/laws/show/2648-20>

7. About the Center for Humanitarian Demining. Ministry of Economy of Ukraine. Available at: <https://me.gov.ua/Tags/Documents/Rozminuvannia>

8. Zablodska, I., Galgash, R., Romakhova, O. (2024). Assessment of the effectiveness and effectiveness of the functioning of communities as a precondition for the reconfiguration of the administrative-territorial structure of Donetsk and Luhansk regions after de-occupation. *Economics and Law*. No1. P. 60–68. <https://doi.org/10.15407/econlaw.2024.01.060>

9. Майбутнє Донбасу. Available at: <https://www.future-east.org/>

10. Draft Law of Ukraine ‘On the Introduction of a Special Regime of Economic Activity in the Territory of Priority Development in Donetsk and Luhansk Regions’. Available at: <https://itd.rada.gov.ua/billInfo/Bills/Card/38491>

11. Draft Law on the War Risk Insurance System. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/55532>

12. Draft Law on Amendments to Paragraph 4 of Section XXI ‘Final and Transitional Provisions’ of the Customs Code of Ukraine on Compensation of Investments through Taxes. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/56645>

13. Draft Law on Amendments to Section XX ‘Transitional Provisions’ of the Tax Code of Ukraine on Compensation of Investments through Taxes. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/56646>

14. Draft Law on Amendments to the Law of Ukraine ‘On Ensuring the Rights and Freedoms of Internally Displaced Persons’ and Other Laws of Ukraine. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/45414>

15. Draft Law on the Principles of State Policy of the Transition Period. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/27539>

16. Draft Law on Amendments to the Law of Ukraine "On Compensation for Damage and Destruction of Certain Categories of Real Estate Objects as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine, and the State Register of Property Damaged and Destroyed as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine" and some other laws of Ukraine on improving the mechanism provision of compensation and accounting of real estate. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/56069>

17. Draft Law on Amendments to Certain Laws of Ukraine to Improve the Legal Regulation of Issues Related to Compensation for Damage and Destruction of Certain Categories of Real Estate Objects as a Result of the Armed Aggression of the Russian Federation against Ukraine and Maintenance of the State Register of Property Damaged and Destroyed as a Result of Hostilities, Terrorist Acts, Sabotage Caused by the Armed Aggression of the Russian Federation against Ukraine. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/44619>

18. Draft Law on Amendments to Certain Laws of Ukraine on Charging for Housing and Communal Services and Accounting for Losses in Connection with Damage or Destruction of Real Estate. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/56128>

19. Draft Law on the Basic Principles of Housing Policy. Available at: <https://itd.rada.gov.ua/billinfo/Bills/Card/55543>

Contributors

ALEKSIN Glib

PhD (Economics), Associate Professor, Corporate finance and Controlling Department, Vadym Hetman Kyiv National Economic University, Kyiv (Ukraine)

***BEDRII
Dmytro***

Doctor of Sciences (Technical), Associate Professor, Senior Researcher, Acting Director, State Enterprise ‘Ukrainian Scientific Research Institute of Radio and Television’, Professor of the Department of Artificial Intelligence and Data Analysis, Odesa Polytechnic National University, Professor of the Department of Management and Marketing, Odesa State Academy of Civil Engineering and Architecture, Odesa (Ukraine)

BONDAR Iuliia

PhD (Economics), Full Professor, Professor of the Department of Management and Entrepreneurship, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, (Ukraine)

BORODINA Oksana

PhD (Public Administration), Senior Researcher, the State Organization ‘V. Mamutov Institute of Economic and Legal Research of National Academy of Sciences of Ukraine’, Kyiv (Ukraine)

BUTS Yuriy

Doctor of Sciences (Technical), Full Professor, Head of the Department of Occupational Safety and Environmental Protection, Ukrainian State University of Railway Transport, Kharkiv (Ukraine)

DEACON Yuriy

PhD (Economics), Researcher of the Department of Interregional Cooperation of the Luhansk Branch of the State Organization ‘V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine’, Kyiv (Ukraine)

DYCHKO Alina

Doctor of Sciences (Technical), Professor, Professor of the Department of Ecology and Environmental Protection Technologies of the National Transport University, Kyiv (Ukraine)

***DZHABRAILOV
Ruslan***

Doctor of Sciences (Law), Full Professor, Deputy director of the State Organization ‘V. Mamutov Institute of Economic and Legal Research of National Academy of Sciences of Ukraine’ Kyiv (Ukraine)

FEDULOVA Svitlana

Doctor of Sciences (Economics), Full Professor, Head of the Global Economy Department, Alfred Nobel University, Dnipro (Ukraine)

<i>HAVRYLIUK Oleh</i>	Doctor of Sciences (Economics), Full Professor, Professor of Marketing Department, Private Institution of Higher Education «European University», Kyiv, (Ukraine)
<i>HLUKHONETS Andrii</i>	PhD (Technical Sciences), Associate Professor, Associate Professor of the Department of Ecology and Environmental Protection Technologies of the National Transport University, Kyiv (Ukraine)
<i>HUDIMA Tetiana</i>	Doctor of Sciences (Law), Full Professor, ~~писати~~ Deputy head of the Department of economic law and legislation modernization Issues of the State Organization ‘V. Mamutov Institute of Economic and Legal Research of National Academy of Sciences of Ukraine’, Kyiv (Ukraine)
<i>HUTSALIUK Oleksii</i>	Doctor of Sciences (Economics), Full Professor, Vice-Rector for Scientific and Pedagogical Activities, Private Higher Education Institution ‘Rauf Ablyazov East European University’, Cherkasy, (Ukraine)
<i>IVANOVA Roksolana</i>	PhD (Law), Associate Professor, Professor of the Department of International and European Law, Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi (Ukraine)
<i>KLIUCHNYK Ruslan</i>	PhD (Political), Associate Professor, Associate Professor of Global Economics Department, Alfred Nobel University, Dnipro (Ukraine)
<i>KRAINIUK Maksym</i>	Postgraduate student, Kharkiv National Automobile and Highway University, Kharkiv (Ukraine)
<i>KRAINIUK Olena</i>	PhD (Technical Sciences), Associate Professor, Head of the Department of Cybersecurity, Kharkiv National Automobile and Highway University, Kharkiv (Ukraine)
<i>KUZMINOV Serhii</i>	Doctor of Sciences (Economics), Full Professor, Professor of the Global Economics Department, Alfred Nobel University, Dnipro (Ukraine)
<i>LEONOVA Sofiia</i>	PhD (Economics), Associate Professor of the Department of Marketing and Logistics, Lviv Polytechnic National University, Lviv (Ukraine)
<i>LUKIANENKO Nataliia</i>	Lecturer, Department of Foreign Languages, Kharkiv National Automobile and Highway University, Kharkiv (Ukraine)
<i>LYASHENKO Pavlo</i>	PhD (Economic), Researcher of the Department of Interregional Cooperation of the Luhansk Branch of the State Organization ‘V. Mamutov Institute of Economic and Legal

	Research of the National Academy of Sciences of Ukraine', Kyiv (Ukraine)
LYMONOVA Elvina	PhD (Economic), Associate Professor, Associate Professor of Global Economics Department, Alfred Nobel University, Dnipro (Ukraine)
MINAIEVA Yuliia	Senior Lecturer of the Department of Engineering Systems and Technologies, V.I. Vernadsky Tavrichesky National University, Kyiv (Ukraine)
MOSTOVA Anastasiia	Doctor of Sciences (Economics), Associate Professor, Associate Professor of the Varna University of Management, Varna (Bulgaria)
NECHYPORENKO Tetiana	PhD (Economics), Associate Professor, Vinnytsia National Technical University, Vinnytsia (Ukraine)
NIKOLENKO Liudmyla	Doctor of Sciences (Law), Full Professor, Leading Researcher of the Department of Economic and Legal Research Problems of Economic Security, State Organization 'V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine', Kyiv, (Ukraine)
PASICHNYK Taras	PhD (Economics), Associate Professor, Department of Foreign Economic Activity Management, University of Customs and Finance, Dnipro (Ukraine)
PETRUNENKO Iaroslav	Doctor of Sciences (Law), Full Professor, Leading Researcher, State Organization 'V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine', Kyiv (Ukraine)
PETRUNIA Yurii	Doctor of Sciences (Economics), Full Professor, Professor of the Department of Foreign Economic Activity Management, University of Customs and Finance, Dnipro (Ukraine)
PRODANYK Vasyl	PhD (Public Administration), Associate Professor of the Department of Public Administration, Educational and Scientific Institute of International Relations and Social Sciences, Private Higher Educational Institution 'Interregional Academy of Personnel Management', Kyiv (Ukraine)
SERGIHENKO Tetiana	PhD (Political), Associate Professor, Associate Professor of the Department of Business and Management, National University 'Zaporizhzhia Polytechnic', Zaporizhzhia (Ukraine)
SHCHEKHOVSKA Larysa	PhD (Public Management and Administration), Associate Professor at the Department of Logistics, State University 'Kyiv Aviation Institute', Kyiv (Ukraine)

<i>SHPAK Nataliia</i>	Head of International Activity Department, Alfred Nobel University, Dnipro (Ukraine)
<i>SKOROBOHATOVA Natalia</i>	PhD (Economics), Associate Professor, Associate Professor of the Department of International Economics, National Technical University of Ukraine ‘Igor Sikorsky Kyiv Polytechnic Institute’, Kyiv (Ukraine)
<i>TARANENKO Iryna</i>	Doctor of Sciences (Economics), Full Professor, Professor of the International Marketing Department, Alfred Nobel University, Dnipro (Ukraine)
<i>USTYMENKO Volodymyr</i>	Corresponding Member of the National Academy of Sciences of Ukraine, Corresponding Member of the National Academy of Legal Sciences of Ukraine, Doctor of Sciences (Law), Professor, Honored Lawyer of Ukraine, Member of the Presidium of National Academy of Sciences of Ukraine, Director of the State Organization ‘V. Mamutov Institute of Economic and Legal Research of National Academy of Sciences of Ukraine’, Kyiv (Ukraine)
<i>VOLOBOIEV Volodymyr</i>	PhD (Economics), Associate Professor of the Department of Entrepreneurship and Management, Zaporizhzhia Institute of Economics and Information Technologies, Zaporizhzhia (Ukraine)
<i>VOROTIN Valerii</i>	Doctor of Sciences (Public Administration), Professor of the Educational and Scientific Institute ‘Public Management and Administration’ of Mykhailo Drahomanov Ukrainian State University, Kyiv (Ukraine)
<i>VOROTINA Nataliia</i>	PhD (Law), Associate Professor, Senior Research Fellow at the Department of problems of public administration and administrative law, V. M. Koretsky Institute of State and Law, National Academy of Sciences of Ukraine, Kyiv (Ukraine)
<i>YATSKEVYCH Inna</i>	Doctor of Science (Economics), Professor, Professor of the department of management and marketing, Odesa State Academy of Civil Engineering and Architecture, Odesa (Ukraine)
<i>ZABLODSKA Inna</i>	Doctor of Sciences (Economics), Full Professor, Director of the Luhansk Branch of the State Organization ‘V. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine’, Kyiv (Ukraine)
<i>ZACHOSOVA Nataliia</i>	Doctor of Sciences (Economics), Full Professor, Professor of the Management and Public Security Department, Bohdan Khmelnytsky National University of Cherkasy, Cherkasy (Ukraine)

<i>ZADOIA Anatolii</i>	Doctor of Sciences (Economics), Full Professor, Professor of the Global Economics Department, Alfred Nobel University, Dnipro (Ukraine)
<i>ZADOIA Oleksandr</i>	PhD (Economic), Associate Professor, Associate Professor of Global Economics Department, Alfred Nobel University, Dnipro (Ukraine)
<i>ZAHORODNIA Alona</i>	PhD (Management), Associate Professor of the Department of International Relations and Political Consulting, Kyiv (Ukraine); Institute of Law and Public Relations, Open International University of Human Development «Ukraine», Kyiv (Ukraine)
<i>ZAKHAROVA Oksana</i>	Doctor of Sciences (Economics), Full Professor, Professor of the Department of Economics and Management, Cherkasy State Technological University, Cherkasy (Ukraine)
<i>ZHYKHAREVA-TOLSTIK Hanna</i>	Lecturer, Zuyd University of Applied Sciences, Maastricht, Manager for Regional Cultural Projects, Ministry of Justice and Security, Amsterdam (The Netherlands)
<i>ZIANKO Vitalii</i>	Doctor of Sciences (Economics), Professor, Head of the Department of Finance and Innovation Management, Vinnytsia National Technical University, Vinnytsia (Ukraine)

Scientific publication

EUROPEAN SECURITY ARCHITECTURE IN THE 21st CENTURY

Edited by Prof. A. Zadoia, Prof. S. Fedulova

Monograph

Electronic Edition

HEI “Alfred Nobel University”
49000, Dnipro, Sicheslavska Naberezhna St., 18.
Phone (056) 778-58-66, e-mail: rio@duan.edu.ua
Certificate ДК № 5309, 20.03.2017