KAPITEL 11 / *CHAPTER 11* [11]
DIGITAL-GREEN TRANSITION AND ECONOMIC SECURITY: EU POLICIES, RISKS AND IMPLICATIONS FOR UKRAINE

DOI: 10.30890/2709-2313.2025-42-05-021

Introduction

The European green transition and digital transformation are key drivers of the European Union's competitiveness and economic security. Global investments in digital transformation are expected to reach almost USD 4 trillion by 2028, reflecting growing business interest in data, cloud solutions and artificial intelligence (IDC, 2025).

The combination of digital and green transitions is economically justified and embedded in EU policy frameworks. In the *Digital Decade Policy Programme 2030*, digital transformation is identified as a key factor in achieving climate neutrality (European Commission, 2024a). The *European Green Deal* highlights the role of digitalisation in reducing emissions, optimising energy consumption and ensuring a circular economy. The *European Green Deal* and the *Fit for 55* initiative underline that cutting emissions by 55% by 2030 requires digital solutions such as smart grids, digital twins, and IoT applications in transport and construction, among others (European Commission, 2019; European Commission, 2024b). The *REPowerEU Plan* also provides for the digitalisation of the energy system to accelerate the shift to renewable sources and increase energy efficiency (European Commission, 2022a).

The main challenge lies in bridging digital skills gaps and introducing digital technologies across all sectors of the economy and society while simultaneously limiting the growth of the energy intensity of digital infrastructure. Rising energy consumption can offset climate benefits and therefore requires comprehensive energy-efficiency measures to sustain the digital sector. Ultimately, this calls for the close integration of the digital and green transitions.

[11]***Authors:*** *Mostova Anastasiia Dmytrivna, Kapiton Alla Myroslavivna, Mishustina Tetyana Serhiivna, Strelchenko Inna Illivna, Taranenko Iryna Vsevolodivna*
Number of characters: *45161*
Author's sheets: ***1****,13*

For Ukraine, the combination of digital and green transformations is of strategic importance as an instrument for post-war recovery, integration into the EU, and strengthening economic resilience. Recent years have shown significant progress in digitalisation. Ukraine has entered the world's top five countries in terms of digital public services, while in 2018 it ranked 102nd (CID Harvard, 2025). Ukraine's inclusion in the *Digital Europe Programme* in 2022 opened up additional opportunities for integration into the EU single digital market (European Commission, 2022g). This advances synergy with the EU's digital-green strategies.

11.1 Impact of Digital Transformation on the EU's Competitiveness and Sustainable Development

Digital transformation is a purposeful process of profound change in an organisation, its business model and value chains through the integration of digital technologies and data. In particular, it is a process of enhancing an organisation's competitiveness by combining IT, computing, communications and connectivity, thereby triggering strategic change (Vial, 2019). Digital transformation has evolved from simple digitisation and digitalisation to a strategic process in which value propositions, customer experience and operating models are fundamentally reshaped (Verhoef et al., 2021).

In EU policy documents, digital transformation is described as a structural transition of the economy and society by 2030, with clear objectives and measurable targets set out in the *Digital Decade Policy Programme 2030*, designed to accelerate and shape a successful digital transformation of the Union. To speed up this transition, EU Member States have on average allocated 26% of Recovery and Resilience Facility (RRF) funding to digital technologies, amounting to a total of €127 billion (European Commission, 2024c).

In 2024, 73% of small and medium-sized enterprises (SMEs) in the EU had achieved at least a basic level of digital intensity (the target is 90% by 2030). The share of companies using artificial intelligence increased to 13.5%, compared with 8% in

2023. The number of ICT specialists reached 10.3 million (about 5.0% of total employment), confirming steady growth but also pointing to a shortage of digital skills in view of the 2030 targets. In 2023, 39% of enterprises used cloud computing services, and 55% deployed at least one of three key tools: artificial intelligence, cloud computing or big data analytics (Eurostat, 2025a; Eurostat, 2025b; Eurostat, 2025c).

11.2 Economic Security of the European Union in the Era of Digital and Green Transformation

The European Union is gradually building a comprehensive architecture of economic security capable of simultaneously supporting the digital and green transformations and protecting critical sectors from contemporary threats. The *European Economic Security Strategy* defines four key areas of risk: vulnerabilities in supply chains, threats to critical infrastructure, leakage of sensitive technologies, and economic coercion by third countries (European Commission, 2023f). This document provides the foundation for integrating economic, security and technological approaches and for subsequent institutional and regulatory measures.

Economic security today occupies a priority place in EU strategies, especially in the context of expanding digital markets. It is not merely protection against threats but the foundation of systemic resilience, competitiveness and strategic sovereignty. In 2025, the European Parliament presented a draft *Economic Security Doctrine*, intended to consolidate previously fragmented instruments (from foreign direct investment (FDI) screening to export controls and supply-chain diversification) into a coherent system (European Parliamentary Research Service, 2025).

Within the EU's external policy dimension, the *International Digital Strategy*, unveiled in June 2025, positions economic security as a key element of digital cooperation with third countries. The main objectives of this strategy are to ensure the resilience of supply chains (for example, for semiconductors), to foster technological partnerships, and to promote global standards based on security and transparency to strengthen digital sovereignty (CEPS, 2025a).

Economic security in the EU today constitutes a comprehensive doctrine encompassing investment screening, strategic autonomy, cyber-resilience, technological competence and international coordination. It remains the foundation for digital and green development as well as for long-term resilience.

11.3 Challenges to EU Economic Security in the Digital Transformation Era

Digital transformation opens up vast opportunities but at the same time creates significant risks that can weaken economic security. The main ones include:

1) Cyber risks and attacks on critical infrastructure. In 2024, there was a 35% increase in major cyber incidents affecting energy, water supply and healthcare systems (ENISA, 2025). These developments prompted the European Union to revise its strategy for threats to critical infrastructure and led to the adoption of the *Directive (EU) 2022/2555 – NIS2 Directive*, which sets new requirements for the cyber-resilience of critical sectors.

2) Dependence on global digital giants (Big Tech). Around 68% of industrial-sector data exchange is carried out through platforms controlled by Big Tech, creating risks of invalidation, access blockage or geopolitical pressure. This concern contributed to the adoption of the *Regulation (EU) 2022/2065 – Digital Services Act (DSA)* and the *Regulation (EU) 2022/1925 – Digital Markets Act (DMA)*, which impose obligations on large platforms regarding competition and transparency.

3) Digital inequality and skills gaps. In 2024, 22% of households in Central and Eastern European regions lacked access to high-speed internet, and 28% of users did not possess basic digital skills, resulting in “digital exclusion” (Eurostat, 2025d). In response, the EU launched the *Digital Decade Skills* programme, which provides training grants, online learning platforms and coordination with national governments.

4) Increased energy demand of the ICT sector. EU data centres consumed 45–65 TWh of electricity in 2022 (1.8–2.6% of total EU consumption), while telecom networks consumed 25–30 TWh. The European Commission projects that demand could rise to 98.5 TWh by 2030 (Joint Research Centre, 2024; European Commission,

2023a; Reuters, 2025b). This requires integrated digital and green policies, such as energy-efficiency requirements under the *Eco-design Regulations* (European Commission, 2023e).

5) Data privacy and risks of uncontrolled algorithmic use. The growing deployment of big data and AI poses significant challenges to privacy. According to *Eurobarometer* (2024), 72% of EU citizens express concern about the processing of their personal data. This has reinforced the implementation of the *General Data Protection Regulation (GDPR)*, in force since 2018, and the adoption of the *Regulation (EU) 2024/1689 – AI Act*, which sets requirements for lawful, transparent, safe and controllable algorithms.

11.4 Regulatory and Financial Instruments for Ensuring the EU's Digital and Economic Security

In the field of regulation, the European Union has adopted a series of legislative acts that create the foundation for the security of the digital economy. The *Directive (EU) 2022/2555 – NIS2 Directive* introduces high standards of cyber-resilience for around 160,000 organisations in 18 sectors (European Parliament, 2022). The *Regulation (EU) 2022/2554 – Digital Operational Resilience Act (DORA)*, adopted in 2025, is a key regulatory instrument for ensuring cyber-resilience. This act harmonises requirements for ICT risk management in the financial sector and ensures its protection against cyber-attacks and systemic failures caused by ICT incidents (EIOPA, 2025). The *Regulation (EU) 2024/2847 – Cyber Resilience Act (CRA)*, adopted in 2024, sets mandatory security requirements for digital products and software based on the "secure by design" principle and provides for penalties of up to €15 million or 2.5% of turnover. The *Regulation (EU) 2024/903 – Cyber Solidarity Act (2025/38)* establishes the European Cyber Shield, a mechanism for joint response to cyber threats, and an EU Cybersecurity Reserve with an initial budget of €36 million for three years (ENISA, 2025). The *Directive (EU) 2022/2557 – Critical Entities Resilience (CER) Directive* complements NIS2 with provisions on the physical resilience of critical entities. In

addition, *EU-CyCLONe*, a network for cyber-crisis management under the NIS2 Directive, provides joint tools for coordinated response. Finally, the *European Cybersecurity Competence Centre (ECCC)* coordinates funding and research activities in the field of cybersecurity, ensuring the EU's technological self-sufficiency.

Regulation (EU) 2024/1183 – eIDAS 2.0 has enshrined the European Digital Identity as a basis of trust in public and private online services. eIDAS 2.0 and the European Digital Wallet make large-scale e-services and the "once-only submission" principle technically and legally interoperable across the EU (EUR-Lex, 2025). The *Regulation (EU) 2023/2854 – Data Act* and the *Regulation (EU) 2022/868 – Data Governance Act (DGA)* set rules for access to and sharing of industrial and IoT data, creating the foundation for smart grids, flexible markets and circular business models (European Commission, 2022b; European Commission, 2023b).

The *Regulation (EU) 2024/1689 – AI Act* introduced risk-based requirements for artificial intelligence systems, establishing a trust framework for high-risk applications in energy, transport and healthcare (EUR-Lex, 2024). An important complement is the *Regulation (EU) 2019/881 – Cybersecurity Act*, which created the European cybersecurity certification scheme EUCC (ENISA, 2024). In addition, the *Regulation (EU) 2019/452 – FDI Screening Regulation*, the *Regulation (EU) 2022/2560 – Foreign Subsidies Regulation*, the *Regulation (EU) 2022/1031 – International Procurement Instrument (IPI)* and the *Regulation (EU) 2023/2675 – Anti-Coercion Instrument* provide protection against economic coercion in the EU.

Due to the growing risk of losing technological advantages, the EU has introduced a 15-month screening of foreign investments (since 2021) in artificial intelligence, quantum technologies and semiconductors, with a final report expected by mid-2026 (Reuters, 2025c). Increasing global competition from the United States and China requires the EU to focus on economic security to strengthen competitive advantages in the digital sector. Digital instruments such as the *Recovery and Resilience Facility (RRF)*, the *Industrial Strategy* and FDI screening help maintain the EU's position in the global economy (CEPS, 2025b).

Investment programmes play a significant role in ensuring economic security. The

Digital Europe Programme has a budget of over €8.1 billion for 2021–2027, of which €1.3 billion is allocated in 2025–2027 for the development of artificial intelligence, cybersecurity, digital skills and key infrastructures (European Commission, 2025). Under the *Cyber Solidarity Act*, the EU Cybersecurity Reserve provides Member States with access to managed security services (ENISA, 2025). The *Connecting Europe Facility – CEF Digital* programme, with a budget of about €2.07 billion, supports the creation of secure 5G corridors and cross-border networks (European Commission, 2022d).

Horizon Europe, within its "Civil Security for Society" cluster, has allocated approximately €1.6 billion for research and innovation in civil security and cyber-resilience (European Commission, 2021c). In addition, the *Chips Act* is mobilising more than €43 billion by 2030, of which €3.3 billion comes directly from the EU budget (European Commission, 2022e). The *Strategic Technologies for Europe Platform (STEP, Regulation (EU) 2024/795)* allows resources from eleven EU programmes to be redirected to critical technologies with co-financing of up to 100% (European Commission, 2024e). Institutional coordination in cybersecurity is ensured by the *European Cybersecurity Competence Centre (ECCC)* and the network of national coordination centres (European Commission, 2021b). The *Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²)* programme, with a budget of around €10 billion, develops secure satellite communications for critical infrastructure needs (European Commission, 2023d).

The interaction of regulatory and financial instruments not only establishes high security requirements but also provides the resource base for their implementation. NIS2, CER, DORA, CRA, eIDAS 2.0 and other acts make cyber-resilience and physical security integral elements of critical sector operations. The Data Act, DGA and AI Act create frameworks for the secure use of data and algorithms in industry, energy and transport. Investment programmes such as Digital Europe, CEF Digital, Horizon Europe, STEP and the Chips Act finance the development of infrastructure, research and production. Mechanisms for screening foreign investment and controlling subsidies strengthen the EU's strategic autonomy in the digital sector and technological

independence.

At the same time, the scale and speed of implementation of these measures remain the main challenge. NIS2 alone extends requirements to approximately 160,000 organisations, while DORA will cover the entire financial sector from 2025. This requires substantial investment by both businesses and governments in security monitoring centres, ICT solution certification and effective supplier management. In view of this, the EU allocated an additional €1.3 billion for 2025–2027 under the Digital Europe Programme, established the EU Cybersecurity Reserve and mobilised over €43 billion to develop the semiconductor industry. However, the risks of bottlenecks in technological supply chains remain, requiring sustained investment coordination and closer cooperation between the public and private sectors.

Thus, instruments of economic and cybersecurity are becoming increasingly integrated into EU policy, forming the basis for sustainable, secure and technologically independent development.

11.5 Synergy of Digital Transformation and the Green Transition as a Driver of EU Economic Security

The European Commission explicitly links digitalisation with the green course. This is reflected in key strategies such as the *European Green Deal*, *Fit for 55* and *REPowerEU*, which directly integrate digitalisation into the achievement of climate objectives. Deep digital modernisation of the energy system is a prerequisite for the integration of renewable energy sources, demand flexibility and system security (EUR-Lex, 2022). Digital technologies are increasingly becoming a catalyst for sustainable development, ensuring efficient resource use, emission reduction, supply-chain transparency and better adaptation to climate challenges. Digital solutions are essential for achieving climate neutrality, improving energy efficiency and creating a circular economy.

The EU has adopted policies and initiatives across every sector of the economy. In the energy sector, the use of smart grids and the Internet of Things (IoT) increases

the resilience of energy systems. Digitalisation of energy can reduce system energy consumption by 10–15% by 2030. Digital solutions for managing demand flexibility contribute to the growing share of renewables (European Commission, 2022a). The *Digitalising the Energy System* programme provides for the creation of a unified *Energy Data Space*, enabling more efficient grid balancing and reducing energy costs for businesses and households (OP Publications, 2023). The European *Destination Earth (DestinE)* initiative creates digital "twins" of the Earth to model extreme weather events and support climate adaptation (ECMWF, 2024).

In the transport and mobility sector, the revised *Directive (EU) 2023/2661 on Intelligent Transport Systems (ITS)* expands the framework for European real-time services and seamless multimodality (European Commission – Transport, 2025a; EUR-Lex, 2023). Digital technologies help reduce emissions by optimising routes and promoting multimodal solutions. The implementation of smart transport systems is expected to reduce road congestion by 15–20% and urban CO_2 emissions by 8–10% by 2030 (European Commission – Transport, 2025a). The creation of the *European Mobility Data Space (EMDS)* will ensure real-time access to transport data, contributing to more sustainable transport (European Commission – Transport, 2025b).

The building sector accounts for almost 40% of the EU's energy consumption and 36% of its CO_2 emissions (European Commission – Energy, 2024). The introduction of smart management systems and digital twins allows optimisation of heat and electricity use, reducing costs by up to 25% (European Commission – Energy, 2020). The revised *Energy Performance of Buildings Directive (EPBD)* makes the *Smart Readiness Indicator (SRI)* mandatory for most new and renovated buildings, stimulating the use of digital technologies for decarbonising the sector (European Commission – Energy, 2024).

In the health sector, the *Regulation (EU) 2025/327 – European Health Data Space (EHDS)* ensures primary and secondary use of e-health data for cross-border diagnostics, research and innovation. The creation of the *EHDS* opens opportunities for data exchange among EU countries, improving access to medical services and supporting scientific research. According to the European Commission, this can reduce

healthcare costs by 5–7% thanks to digital diagnostic and monitoring tools.

In the industrial sector, digitalisation supports the transition to circular business models. The *Regulation (EU) 2024/1781 – Ecodesign for Sustainable Products Regulation (ESPR)* introduces the *Digital Product Passport* for all products placed on the EU market, enabling tracking of their life cycle and promoting material reuse. Joint European data spaces (industrial, green, energy and others) create the infrastructure for trusted data exchange. In automotive supply chains, inter-company exchange of production and environmental data is being implemented, ensuring transparency of the carbon footprint (Catena-X, 2025).

Thus, digital technologies not only increase productivity and efficiency but also create the conditions for achieving climate neutrality and economic resilience. At the same time, they require control over the growing energy consumption of digital infrastructure to ensure that the digital transition reinforces the green transition.

The digital-green synergy also has an economic security dimension. The use of open data, artificial intelligence and digital platforms enables more effective monitoring of emissions, resource management and supply-chain control. At the same time, the security of digital infrastructure becomes a critical precondition for achieving climate objectives.

In conclusion, the synergy of digital transformation and the green transition lies in the mutual reinforcement of both processes. Digital technologies become a key instrument for achieving climate neutrality, while the green course provides incentives for the development of innovative digital solutions. This interconnection forms the foundation for a sustainable and secure economic future of the European Union.

11.6 Impact of Digital and Green Transformation on Ukraine's Recovery and Economic Security

For Ukraine, the combination of digital and green transformations is of priority importance. This synergy is part of post-war recovery and integration into the European Union and at the same time an instrument for strengthening economic resilience and

energy independence. Ukraine has made significant progress in the digital sphere. In 2022, the country joined the *Digital Europe Programme*, gaining access to the EU single digital market and to joint projects in cybersecurity, digital innovation and skills development (European Commission, 2022g). A notable example is the Diia platform, used by more than 22 million citizens and providing over 140 electronic services. This tool has ensured not only convenience but also the resilience of public administration during wartime, confirming Ukraine's potential as a digital partner of the EU (VoxUkraine, 2025).

At the same time, the country is actively developing the green transition despite the devastating consequences of the war. The share of renewable energy in total energy consumption increased from 3.9% in 2014 to 9.2% in 2020 (Wikipedia, 2025). National companies are shaping large-scale investment strategies. In particular, the "30 GW by 2030" strategy provides for large private investments in renewable energy of around €35–40 billion. The company DTEK has already invested more than USD 1.2 billion in solar and wind power plants, including the Tylihul Wind Power Plant (Tylihul WPP) with a capacity of 114 MW in Mykolaiv region (Wikipedia, 2025).

International partners are also actively involved in projects. In 2025, the joint project of Octopus Energy and DTEK envisages €100 million of investment to create up to 100 solar and battery storage systems using artificial intelligence to optimise consumption (Reuters, 2025a). A study of rooftop photovoltaic potential shows that Ukraine can install up to 238.8 GW of rooftop solar panels, providing about 290 TWh of electricity per year and enabling the creation of a decentralised and resilient energy system (Winkler et al., 2024).

The combination of digital and green innovations creates not only domestic opportunities for Ukraine but also enhances its foreign-policy role. Digital transformation builds the infrastructure for integration into the EU's digital and green space. It enables transparent resource management, monitoring of reconstruction and control of financial flows. During the war, data from unmanned systems, artificial intelligence and cybersecurity became a strategic competitive advantage, turning Ukraine into an important digital partner of the West (Reuters, 2025d). Thus, the "dual

transition" in Ukraine is not only a technological or energy strategy but also a comprehensive model of recovery and integration based on economic resilience, climate responsibility and innovation.

Therefore, economic security has become a strategic priority for the EU, shaping the logic of digital and green transformation. The synergy of digital and green transitions provides the EU with a unique opportunity to combine economic development with climate objectives, making innovation an instrument of resilience. For Ukraine, this experience is of critical importance, as the dual transition becomes not only a condition for integration into the EU but also a model for recovery and long-term economic security.

Conclusions and Policy Recommendations for Ukraine

Digital transformation is becoming a critical factor for the sustainable and secure economic development of the European Union. It not only supports the competitiveness of the internal market but also forms the basis for strategic autonomy and economic security. The adoption of key legislative acts confirms that digitalisation is already integrated into the broader security dimension of the EU.

The synergy of digitalisation and the green transition shapes a new model of European competitiveness. Digital technologies are becoming a necessary condition for achieving climate goals, while the green course creates incentives for the development of innovative solutions in energy, transport and industry. This dual transition strengthens economic resilience, ensures control over strategic resources and reduces dependence on external suppliers.

For Ukraine, integration into European policies in the field of digital and green transformation is not only a strategic objective but also an opportunity to take advantage of recovery prospects. Accession to the *Digital Europe Programme* and the implementation of large-scale renewable energy projects demonstrate the country's ambition to synchronise with the EU and at the same time enhance its own resilience.

To maximise the benefits of the dual transition, Ukraine needs to invest in the

development of digital skills, which are the foundation for innovative growth; ensure the cyber-resilience of critical sectors; support innovative ecosystems that bring together business, science and the state; and strengthen partnership with the EU in the sphere of the dual transition. Only a comprehensive implementation of these areas can ensure sustainable, secure and competitive development for both the EU and Ukraine.

For Ukraine, the digital-green transformation should become a key driver of recovery, integration into the EU and the strengthening of economic security. The EU's experience shows that the combination of digital technologies and the green economy creates a powerful multiplier effect, simultaneously increasing productivity, energy efficiency and innovation capacity (European Commission, 2019; European Commission, 2022a).

First, it is necessary to invest in the development of digital skills and digital education. As of 2023, only about 54% of Ukrainian citizens had basic digital skills, while the EU average exceeded 70 per cent (Eurostat, 2023). This gap may become a barrier to full integration into the European digital space; therefore, state policy should include large-scale educational programmes and support for reskilling initiatives.

Second, strengthening the cyber-resilience of critical infrastructure must be a priority. Ukraine's participation in the *Digital Europe Programme* and the *EU Cybersecurity Reserve* (ENISA, 2025) should be complemented by the creation of its own Security Operations Centres (SOC), certification mechanisms and integration into the European system for incident data exchange. This will help reduce the vulnerability of the economy to external threats.

Third, the green transition should become the basis for energy independence and the reduction of dependence on fossil fuel imports. Ukraine already has an ambitious "30 GW by 2030" strategy, but its implementation requires access to EU investment instruments, in particular *InvestEU* and the *Just Transition Mechanism* (European Commission, 2021a; European Commission, 2020). The development of decentralised energy, including rooftop photovoltaic installations, is of particular importance.

Fourth, it is necessary to support innovative ecosystems that unite business, science and government institutions. The integration of Ukrainian companies and start-

ups into *Horizon Europe* and *EIT Digital* programmes creates opportunities for the development of solutions at the intersection of digital and green technologies, from smart-grid systems to AI-based production optimisation.

Finally, strategic partnership with the EU is of critical importance. Participation in digital and climate initiatives should be complemented by political dialogue on Ukraine's integration into the EU internal market in the areas of energy, digital services and data protection. This will not only strengthen resilience but also ensure Ukraine an active role in shaping the future model of European economic security.

Funding

The paper is based on the results of research conducted under the project Erasmus+ Jean Monnet "EU strategies for competitiveness, growth and prosperity" for study programmes in Alfred Nobel University" № 101085347 — EUSTRAT — ERASMUS-JMO-2022-HEI-TCH-RSCH. Funded by the European Union. Views and opinions expressed are however those of the author 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.